THE RESILIENT HOMELAND: BROADENING THE HOMELAND SECURITY STRATEGY

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

MAY 6, 2008

Serial No. 110–110

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

42–876 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

CONTENTS

THE RESILIENT HOMELAND: BROADENING THE HOMELAND SECURITY STRATEGY

Tuesday, May 6, 2008

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 10 a.m., in Room 311, Cannon House Office Building, Hon. Bennie G. Thompson [chairman of the committee] presiding.

Present: Representatives Thompson, Harman, Lowey, Norton, Jackson Lee, Christensen, Etheridge, Cuellar, Carney, Green, Pascrell, King, Lungren, Rogers, Reichert, Dent, and Miller.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

I would like to thank Ms. Jackson Lee for agreeing to tentatively step in in place of the Chair in case my flight did not get in, but believe it or not, we got in on time.

Thank you very much, Ms. Jackson Lee, for agreeing.

The committee is meeting today to receive testimony from the Department of Homeland Security and from key stakeholders to better understand their efforts to communicate, to coordinate and to collaborate on resilience as a critical part of their mission and operation.

I would like to welcome this panel of esteemed individuals who are here to testify before the Committee on Homeland Security about resiliency.

As the world becomes increasingly more flat, a primary distinction between a competitive nation and those nations left behind will be a nation's resilience. "Resilience" is commonly defined as the ability to recover or adjust easily to misfortune or to change. As it relates to the Department and its functions, resilience is a practice which will allow a quick return to effective, if not 100 percent normal, operations in the wake of an attack or a disaster. Today, we will hear from key partners on this issue—the private sector, one of the country's busiest airports and a leading airport—on resilience.

Our Nation's success is in the hands of our critical partners, and we have a role to play. Of the Nation's critical infrastructure, 85 percent, is owned or operated by the private sector. The business community must have cutting-edge technology in order to effectively bounce back. Colleges and universities must provide sound research on the latest technologies and must develop curricula to train the next generation of homeland security experts.

Under my leadership, the committee has taken steps to further the resilience of our Nation's critical infrastructure. Understanding that we all have a role to play, this committee has taken the lead on making the necessary legislative changes.

Earlier this year, the committee adopted and reported out the Chemical Facility Antiterrorism Act of 2008, which included the promotion of inherently safer technology to lower the possible consequences of an attack or of an accident at a facility. Last year, H.R. 1, or the 9/11 bill, was signed into law, and it included a title that promotes the Private Sector Preparedness Voluntary Certification Program, which encourages stakeholders to adopt standards that ensure effective continuity. Just last week, the Subcommittee on Emergency Communications, Preparedness, and Response marked up H.R. 5890, the Citizen and Community Preparedness Act of 2008, a bill that supports citizen preparedness, which is the cornerstone of a resilient homeland.

On the other hand, since 9/11, this administration has focused solely on preventing the next attack as opposed to how best to recover should an incident occur. That, of course, is not the best approach. We must ensure that the Department is properly communicating, collaborating and coordinating with key stakeholders and critical partners to make sure that we, as a Nation, are prepared for what to do after an attack.

Resilience offers an effective metric: time. We know that companies can measure how long they will be down in the wake of a particular disaster and can work to minimize that time. So it makes sense that the ability to measure downtime makes resilience a good security policy. Simply put, the longer our economic sector is down, the more the terrorists will brag that they are successful.

I know that resilience is not universally applicable, but where it is resilient, the Department must promote resilience.

In closing, promoting resilience requires honesty with the American people. It is through that honesty that we can provide this Nation's citizens with freedom from fear. It also ensures the involvement of critical stakeholders and keeping America strong.

The Chair now recognizes the ranking member of the full committee, the gentleman from New York, Mr. King, for an opening statement.

Mr. KING. Thank you, Mr. Chairman. I am glad you made your plane. It is always good to have you here.

Very seriously, I want to thank you for holding this hearing. Obviously, resiliency is an important component of the whole homeland security effort. As you pointed out in your remarks, 85 percent of the infrastructure—of the critical infrastructure, is privately owned; and that is probably what separates or that is probably the largest distinction between homeland security and the traditional overseas threats we face.

Until September 11, certainly our concept of security was that we would have the military protect us, and it was primarily an overseas operation, done through the Defense Department. With Homeland Security, we realize how much of a factor not just local governments have but also private industry, the private sector. You are right, resilience is absolutely essential if we are to prevail against terrorism in all its forms. Of course, the longer we are

down, the greater the victory it will be for an Islamic terrorist attack.

Now, certainly in New York, we have seen resiliency. We saw the police and firefighters after September 11. We saw the New York Stock Exchange open within approximately 1 week of the attacks on the World Trade Center. We saw the clearing of the area at Ground Zero in less than 8 months when people were projecting 2 years, but the fact is, more can be done, more must be done.

I know the Department of Homeland Security works within the whole concept of continuity of government. Certainly we in the Congress have to work also on the continuity of government. There are so many elements to this, as to how long it can take us and the various sectors to bounce back as quickly as possible.

So I look forward to the testimony.

I want to especially, on a side note, thank Secretary Baker for the work he has done lately as far as certain 9/11 victims in New York. It took a lot of guts and ingenuity on your part. I truly appreciate that, and I will do all I can to support your efforts as we go forward.

With that, I yield back, and I look forward to the testimony.

Chairman THOMPSON. All members of the committee are reminded that, under committee rules, opening statements may be submitted for the record.

[The statement of Hon. Jackson Lee follows:]

PREPARED STATEMENT OF HON. SHEILA JACKSON LEE

As we approach the 7-year anniversary of the attacks on September 11, 2001, and the 3-year anniversary of Hurrican Katrina, one of the most devastating hurricanes in our Nation's history, and reflect upon the Federal Government's response, I think it is a very appropriate time to critically re-examine our capacity for response, recovery, and resilience.

Of the Nation's critical infrastructure assets, 85% are owned or operated by the private sector. Furthermore, a February 2006 report entitled "The Federal Response to Hurricane Katrina: Lessons Learned" states that the Federal Government should recognize that the private sector often performs certain functions more efficiently and effectively than the government because of the expertise and experience in applying successful business models. Thus, the private sector plays an integral role in our resilience efforts.

However, we also need to hear from DHS because we cannot only rely on private solutions to public harms. The government should not abrogate its responsibility over the general welfare of its citizens, and all levels of government (Federal, State, and local) must do a better job of coordinating and ensuring that recovery, response, and resilience efforts are made and delivered in a more comprehensive and efficient manner in the wake of attacks, disasters, or disruptions. DHS must lead the effort to implement policies which mitigate the effects of an attack, disaster, or disruption and ensure that people, systems, and assets are operating effectively immediately after such an eventuality.

Chairman THOMPSON. Let me at the outset ask that, if you have a cell phone, please put it on vibrate or Mr. Twinchek is authorized to handcuff whoever's phone rings and will drag him out of the committee room. Please, honor our rules. Phones are not to be on audible, and we will hope that you will respect the rules.

I welcome our panel of witnesses. Our first witness, the Honorable Stewart Baker, is Assistant Secretary for Policy at the Department of Homeland Security. Mr. Baker will discuss how the Department is promoting resilience and is communicating, coordinating and collaborating with critical stakeholders.

Our second witness, Dr. Yossi Sheffi——

Mr. SHEFFI. Close enough.

Chairman THOMPSON. Close enough? All right—is a Professor of Engineering at the Massachusetts Institute of Technology. He is an expert in promoting resiliency, who will discuss the importance of investing in resilience, which can result in heightened security and can help stakeholders gain an economically competitive advantage.

Our third witness is Erroll Southers, Chief of Homeland Security and Intelligence, Los Angeles World Airports Police Department. Chief Southers will demonstrate how local governments are implementing policies of resilience to ensure the continuity of operation.

Our fourth witness is Dr. Susan Bailey, Vice President of Global Network Operations Planning, AT&T. Dr. Bailey will outline how her company's approach to protecting its network and in responding to disasters is a best practice model.

Our fifth witness is Mary Arnold, Vice President, Government Relations, SAP America. Ms. Arnold will broadly discuss resilience and the global supply chain.

The committee is pleased to have you here as our panel of witnesses. Without objection, the witnesses' full statements will be inserted in the record.

I now recognize each witness to summarize their statements for 5 minutes, beginning with Assistant Secretary Baker.

STATEMENT OF HON. STEWART A. BAKER, ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY

Mr. BAKER. Thank you, Chairman Thompson, Ranking Member King and distinguished members of the committee. I am pleased to appear before you today to talk about how the Department of Homeland Security can build a resilient homeland.

Everyone, I believe, understands the Department's primary mission to be preventing acts of terrorism; we must make every effort to stop an attack. But I think everyone also recognizes that that is not enough. We have to do more. We have to recognize that stopping every terrorist attack may not be possible, and certainly, we are not going to stop every natural disaster. That means that we have to be prepared.

We have to plan for and be prepared for what happens the day after, the hour after, the minute after an attack or a natural disaster. We have to be prepared in a way that allows us to bounce back quickly from the consequences of the attack or the disaster. That is "resilience," and it is a vital part of our mission as the Department of Homeland Security.

I want to begin by giving credit to the committee for having a hearing on this topic. It is an absolutely essential topic. It is one that should inform every aspect of the Department's policy, and it is not something that receives attention every day. We are looking forward to the month of hearings that will address these issues across the board at the Department.

As we have thought about how to promote resilience, at least in the Department, we have begun with what we think are our strengths as a Nation. We are a free and independent people, and we are served by a free market, and those actually turn out to be the central elements of a resilient response to disaster. There is no

government in the world that can respond as creatively and as quickly as individuals who are concerned with the well-being of their families, of their businesses and of their communities. What we need to do as a government is to play a role that allows those individuals, that allows those businesses to respond quickly and creatively on their own to disasters, but in a framework that we have created that will encourage creativity and will give people the tools that they need to respond.

So, as we have thought about resilience, we think of it in terms of providing tools, including new technologies, to individuals and businesses so they can respond creatively as individuals and businesses; and second, creating the kind of order and infrastructure that allow people to focus on the response to the disaster and not on self-protection, not on simply trying to make their telephones work.

I will give just two examples of the kinds of things that we think contribute to resilience; and then, of course, after the opening statements, I will be glad to elaborate in response to questions.

Information: The kinds of information that people need to respond on their own, and creatively, to disasters, I think was vividly illustrated during the California wildfires that we had just recently when the government used reverse 911 to send warnings to people, based on where their homes were, about the progress of the fires so that they could send them evacuation messages that were tailored specifically to where they were. That is the taking of technology we are very familiar with, 911, flipping it around and using it to send messages to people so they can evacuate on their own instead of the government's taking responsibility for trying to evacuate each person. Reverse 911 is, I think, just an example of the kinds of technologies that we can make available to people in a disaster that will allow them to respond much more flexibly.

The other kinds of technologies that we are hoping to bring to bear to foster resilience include instant messaging, short message service—SMS texting, it is called, for those of you who do not have teenage children—geographic information systems and video, Google maps, and Twitter—blogging by cell phone. All of those are tools that, in an emergency, can help people respond, to understand where the danger is, what kinds of responses are available and that can allow them to quickly self-organize and self-rescue.

The government also, I think, has a role—in addition to sponsoring some of these new technologies—in providing the infrastructure of order and the basic communications techniques that people will need in order to most effectively self-organize and self-rescue.

I think we all remember many of the difficulties that were faced during the Katrina effort, to recover from Katrina, and the concerns that were raised by public order breakdowns and the extent of the effort that people put into protecting themselves from what were thought to be breakdowns in order. We are looking at the possibility—and I have asked the Assistant Secretary for State and Local Law Enforcement to look at it—of using volunteers from other State and local law enforcement agencies to come to the rescue of neighboring jurisdictions that need urgent assistance.

I will stop there, and I will be glad to answer questions.

Chairman THOMPSON. Thank you. We will allow you to elaborate during the question and answer period.

[The prepared statement of Mr. Baker follows:]

PREPARED STATEMENT OF STEWART BAKER

MAY 6, 2008

Chairman Thompson, Ranking Member King, and distinguished members of the Committee, I am pleased to appear before you today to discuss how the Department of Homeland Security (DHS) can build a resilient homeland.

RESILIENCE

Stopping terrorism is a key mission of the Department of Homeland Security. We must make every effort to prevent an attack, but we must do more. As a Nation, we must be able to withstand a blow and then bounce back. That's resilience.

Along with planning and preparation, resilience is a part of our approach to homeland security. Resilience is stressed in the administration's recently-released, second-generation *National Strategy for Homeland Security*, as well as the National Response Framework and the National Incident Management System. Resilience—of our people, our infrastructure, our economy, our entire Nation—is an essential element of ensuring the safety and security of the homeland.

Some say that we need to characterize our national efforts to secure the homeland as "resilience," as opposed to "preparedness," or even "homeland security." We should not spend too much time on a purely semantic argument, but there is no doubt that resilience—described by some as our ability to "bend but not break," or the ability to absorb the impact of a catastrophe without losing the capacity to function—represents an important dimension in our security efforts.

A focus on resilience has value in part because it forces us to acknowledge the limits of government capability. It requires us to admit that some disasters cannot be avoided. It also requires us to acknowledge that, faced with disaster, most of our citizens, businesses, and other institutions will take action to rescue themselves and others. No government can respond as quickly and as creatively as individuals concerned with the well-being of their families, their businesses, and their communities. That is the source of our resilience as a country. While government plays a crucial role as well, perhaps its most important role is creating conditions that allow the creativity and ingenuity of individuals and businesses to flourish.

At the end of the day, building a resilient homeland requires us to trust our citizens. We must inform them—and trust them to inform others. We must equip them with the right tools and technologies—and trust them to use those tools to help themselves and others. I would like to highlight three concrete ways in which the Federal government is creating conditions that foster national resilience: (1) Disseminating information that allow individuals to act quickly and wisely; (2) maintaining order; and (3) ensuring the availability of a core infrastructure that individuals will rely on. For the remainder of this testimony, I will offer examples, based on past and present threats, of ways that DHS is creating these three preconditions for a resilient Nation.

INFORMATION

Ordinary American citizens are our strongest asset in protecting the Nation and ensuring our common security. In order to maximize this potential, however, citizens need information so they can make informed decisions. We can unlock powerful, self-organizing responses to disasters if we can get good information to individuals quickly. New technologies are creating new ways to deliver good information about disasters to the people who need it most. Our job is to identify these technologies and deploy them where they will do the most good.

When confronted with emergencies or natural disasters, such as the wildfires that raged through San Diego and Los Angeles counties last October or the tornadoes that hit the southern United States, residents often dial 911 as their first course of action. They are seeking timely and accurate information. There's nothing new about that. But national reverse 911 capability is new, and it is the kind of technology that fosters resilience. Developed by a private company, Reverse 911 uses a combination of database and GIS mapping technologies to deliver outbound warnings to communities and organizations at risk. Reverse 911 played a key role in rescue efforts during the California fires. Automated alert messages were sent to thousands of people simultaneously, warning those who were in the path of rapidly ad-

vancing fires. Those citizens then took informed action on their own, providing greater resilience in the face of the threat.

A number of Federal agencies, including DHS, the Department of Transportation, and the Federal Communications Commission, are working on initiatives to make 911 systems more robust, with ability to seamlessly link in advanced technologies with better backup capacity and recovery capabilities. "Next Generation E911" refers to the technologies, such as voice over IP (VOIP); instant messaging, short message service messaging, Wi-Fi, geographic information systems and video, that will allow a broader array of interconnected networks to comprehensively support emergency services—from public access to those services, to the facilitation of those services, to the delivery of the emergency information to dispatchers and first responders.

A resilient response depends not just on individual citizens but on businesses. If disaster strikes a major refinery in the United States, we could rely on government agencies in Washington to divert supplies from elsewhere to cover the needs of the stricken refinery's customers. Or we could rely on the marketplace to make the adjustments that are needed.

In most cases, the marketplace will be more adaptive and more resilient than a response that depends on government. But, like individuals, businesses are likely to need information that is in the hands of government. To create the conditions for resilience, government needs to communicate reliable, timely, and factual information to businesses. That is the goal of *Ready Business*, part of the Department's *Ready* campaign, a national public service advertising campaign designed to educate and empower Americans to prepare for and respond to emergencies. *Ready Business* provides guidance to small- to medium-size businesses regarding which tools and resources are necessary to plan to stay in business, talk to their employees, and protect their investment.

In preparing for incidents that might affect the flow of trade across our borders, the Department has worked with the private sector through venues like the Commercial Operations Advisory Committee and the Trade Support Network to collect information on what the trade community needs to know to make decisions following an incident that affects the flow of trade. U.S. Customs and Border Protection (CBP) created a web-based communication framework to ensure that we can get pertinent information to stakeholders as soon as it becomes available. It is called the Unified Business Resumption Message and it is available on the CBP website as well as via Remote Subscription Service. While this message template was originally created for the land environment, it has now been tailored to specific modes and there are six live websites for northern and southern border highway and rail, air and maritime. This message is also available through List Serve e-mail based messaging, which sends mode specific messages to the e-mail subscriber.

Sometimes the information people need is not about a fast-moving crisis; sometimes they need information about how to prepare for a particularly dangerous new risk. For instance, there are biological risks, natural or manmade, that fall outside the ordinary experience of the American public. If we expect the public to respond creatively and effectively to these risks, we need to give them the information they need about the risk.

At the same time, biological risks are a classic example of a problem that requires a responsible, resilient response by individuals. Relying entirely on government to address the risk is the opposite of resilience.

Let me explain by looking at a biological risk that is of particular concern—an anthrax attack. If the United States suffers an aerosolized anthrax attack, a few hours could make a tremendous difference in the attack's magnitude. Studies indicate that the most prudent response to such an attack is for those who were exposed to take ciprofloxacin or doxycycline.[1] [2] [3] If that is done within 48 hours of exposure, practically everyone will recover. After two days, though, every day of delay means additional casualties. In fact, if medication is delayed by five days, a large majority of those who were exposed will die. So we need to get medicine into our citizens' hands almost immediately after an attack.

---

[1] "Public Health Response to an Anthrax Attack: An Evaluation of Vaccination Policy Options"; Prasith Baccam and Michael Boechler, Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science, vol. 5, no. 1, 2007, pp. 26–34.

[2] "Emergency Response to an Anthrax Attack"; Lawrence M. Wein, David L. Craft, and Edward H. Kaplan, Proceedings of the National Academy of Sciences, April 1, 2003.

[3] "Systematic Review: A Century of Inhalational Anthrax Cases from 1900 to 2005"; Holty, Bravata, Liu, Olshen, McDonald, Owens, Annals of Internal Medicine, American College of Physicians, February 21, 2006, vol. 144, no. 4, pp. 270–280.

What is a resilient response to this problem? Not, I submit, a response that depends entirely on government. Any response that completely relies on the government to distribute medicine to people is fragile. Every organizational failure—every delay in delivering the medicine, every confusion about who will take which pallets to which distribution centers, every miscommunication about where citizens should go to get their supplies—could result in loss of life. That is the opposite of resilient. Instead, we need to provide citizens with the information they need to respond individually and responsibly to the threat. To the extent possible, we need to encourage citizens to prepare in advance by responsibly maintaining their own supply of cipro or doxy for use in an anthrax emergency.

There are risks in an approach that trusts citizens to treat such a supply responsibly. Overuse of antibiotics has severe public health consequences. But so would an aerosolized anthrax attack. DHS is working with Health and Human Services (HHS) to identify the best options for making sure that public citizens, first responders, and federal employees have cipro/doxy in case of an aerosolized anthrax attack. We are considering all options, including an FDA-approved emergency home medical kit, but that might be several years down the road.

ORDER

Resilience also depends on our ability to maintain order. If our citizens do not have confidence that they will be safe, that social order will be maintained, then their energies will be concentrated on protecting themselves from a breakdown in social order and not on responding to the disaster itself. The more confident Americans are in government's ability to ensure order, the more resilient our society becomes.

As our *National Strategy for Homeland Security* explains, we are continuing to develop and strengthen comprehensive and effective continuity programs to ensure the preservation of our government under the Constitution and the continuing performance of national essential functions—those government roles that are necessary to lead and sustain the Nation during and following a catastrophic emergency. A national approach to continuity also requires that State, local, and Tribal governments work to ensure that they are able to maintain or rapidly resume effective functioning during and after catastrophic incidents and are able to interact effectively with each other and the Federal Government. Likewise, we strongly encourage the private sector to conduct business continuity planning that recognizes interdependencies and complements governmental efforts—doing so not only helps secure the United States, but also makes good long-term business sense for individual companies. Such integrated and comprehensive planning is essential to protecting and preserving lives and livelihoods and maintaining our robust economy during crises.

In many cases, local and State forces are entirely sufficient to maintain order in the midst of a disaster. But some disasters will strain those resources past the breaking point. To address that problem, as directed by Congress, we are studying the efficacy of establishing specialized law enforcement deployment teams (LEDTs) from neighboring jurisdictions who would be available to assist State, local, and tribal governments in responding to natural disasters and acts of terrorism. We know that the best people to assist State and local law enforcement in restoring and maintaining order are other State and local law enforcement officers. These LEDT teams could be designed to help avoid the confusion that resulted when law enforcement agencies from around the country responded to Hurricane Katrina in an unorganized manner. Without a coordinating mechanism, Louisiana and New Orleans law enforcement teams were forced to deploy out-of-State law enforcement units "on the fly" rather than requesting the specific teams they needed. LEDTs could help provide an organized system that would allow State and local law enforcement to assist each other in quickly resuming normal police services to an area hit by a terrorist attack or natural disaster.

INFRASTRUCTURE

Finally, the ability of individuals to respond quickly to crises will be greatly enhanced if they can rely on certain core infrastructure.

An old way of thinking about ensuring the ability of key infrastructure to survive terrorist attacks or natural disasters involved investing in redundant and duplicative infrastructure. As noted in our updated homeland security strategy, however, we must instead focus on the resilience of whole systems—an approach that centers on investments that make systems better able to absorb the impact of an event without losing the capacity to function. While this might include the building of redundant assets, resilience is often attained through the dispersal of key functions across multiple service providers, flexible supply chains, and related systems.

No infrastructure is more important to a resilient, self-organizing response than telecommunications and information networks. To build a resilient response, we need to make sure that these networks continue to function in a crisis.

Take the example of a pandemic and dangerous influenza. We know that one is almost certain to strike again, though we don't know when. The pandemic of 1918 had a larger impact on the population of the United States than any other single event in the twentieth century. One of the lessons we learned from that pandemic was the value of social distancing. Those communities with the most disciplined social distancing regimes exhibited the lowest overall mortalities. Social distancing may be even more important in a future pandemic.

Information networks can make social distancing more practical. Telecommuting via the Internet will allow Americans to keep the economy functioning while avoiding crowds and contagion. However, for technology-enabled distancing to work, information technology infrastructure must have the capacity to support a large number of telecommuters. We must also consider how to ensure that the network's bandwidth is not oversubscribed in an emergency.

We must also make sure that the infrastructure can withstand attacks made over our networks. DHS understands that determined and well-resourced cyber adversaries can find their way into most networks. Improving the resilience of private industry and the government to limit the duration and mission impact of successful attacks or cyber incidents is thus a core component of our overall strategy.

Currently, DHS and the Department of Treasury are working with the Financial Services Sector Coordinating Council Subcommittee for Research and Development, along with ChicagoFIRST, an organization dedicated to improving the resilience of financial infrastructure in Chicago, to develop a risk management tool for the finance sector. This tool is designed to help create a computer simulation of a financial enterprise and its value chains, and how different financial institutions interconnect with others.

Once it is finalized, the tool will allow organizations to create and run multi-party disruption scenarios tailored to their individual business models, using their own proprietary data as well as generic data for the rest of the financial sector. In this way, they can find out specifically how a cyber security event or attack will affect not only their own business, but also learn how the responses of other institutions (including the government) might impact themselves, other in their value chain, and in the sector at large. This improves resilience because it helps ensure all institutions that share a common cyber security incident will make informed response decisions that solve the problem with as little negative impact on the sector as possible.

No single financial company would build such a tool and share it with competitors. However, because of support from DHS, the entire financial sector will be able to improve its resilience by being able to assess and protect itself against emerging cyber security threats.

CONCLUSION

As stated in the second-generation *Strategy*, "Recognizing that the future is uncertain and that we cannot envision or prepare for every potential threat, we must understand and accept a certain level of risk as a permanent condition." Ensuring our Nation's resilience in the face of all threats is an essential element of our risk mitigation strategy. Our citizens are resourceful and creative in responding to disaster. We need to give them the tools that allow them to use that creativity—good information, social order, and a functioning communications network.

Chairman THOMPSON. I now recognize Dr. Sheffi to summarize his statement for 5 minutes.

STATEMENT OF DR. YOSSI SHEFFI, PROFESSOR OF ENGINEERING, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Mr. SHEFFI. Thank you very much, Mr. Chairman. Thank you very much, committee members.

I define "resilience," as was just mentioned, as the ability to bounce back from large-scale disruptions. My comments are based on a large research project at MIT, of 4 years, that resulted in a book called the Resilient Enterprise, that mainly looked at how companies should plan and should work toward bouncing back

from large-scale disruption and how their supply chains should bounce back.

Before we talk about it, I really have kind of divided all types of disruption into random events—earthquakes, hurricanes, accidents, acts of negligence and, finally, intentional disruptions. Intentional disruptions, of course, are terrorism, but one can learn a lot from industrial action, from sabotage, from lots of other actions when there is a smart adversary on the other side, because those are different. We can talk about why in a minute.

Some of the compounding effects when you have large-scale disruptions are—first, in many of these cases, there is public fear. If you think about 911, if you think about SARS, if you think about Chernobyl, you know they are issues of public fear which sometimes lead—this may be less popular here—to wrong government reaction, government reaction that exacerbates the situation—not always, of course, but in many cases. Again, we can talk about many examples from other countries from the United States, where government reaction actually made a situation worse.

Two more points: We live in a connected world, and its disruptions usually promulgate very quickly throughout the Nation, throughout the world.

Finally, I just want to say that what the probability usually for a specific disruption or for a specific day or for a specific point is very small when one runs a global enterprise like General Motors or Procter & Gamble or Intel.

The probability that something happens sometimes is not small at all; it is pretty significant. That kind of leads to the whole notion of resilience. It will happen. It does happen. The question is how to respond.

The first step, of course, as was mentioned, is trying to avoid a disruption in the first place. This was the focus of the Department of Homeland Security's specifically looking at terrorist attacks, but if you talk about, you know, random events and accidents, the whole idea there is resilience, how to bounce back, because one can hardly influence the probability or the likelihood of a hurricane's hitting. The question is how to respond to this.

In some sense, we are starting to shift our thinking about intentional disruption, like terrorism, to exactly the same mode of thinking. Some of this will happen. How do we respond?

It does not have to happen in the homeland. The homeland will be affected by a large-scale disruption of supply chains. It can happen in many other places—in a large port, in a large airport, anywhere in the world.

The second step is, of course, implementing a detection system. One thing that was not mentioned—I mean, the worst disruption is not what people think about, a nuclear holocaust, but it is a disruption when the organization under attack does not know that they are under attack until it is too late. Think about a biological agent, a chemical agent, that does not reveal itself until enough people are affected.

Basically, when you think about disruption, you think about two ways to prepare for a response. The first one is redundancy; the second is flexibility. Those are really the only two classes of actions that one can take.

Redundancy is having extra inventory, extra capacity, an extra of something. It is an expensive way to do it, but we do it in many cases.

The other way to think about it is to build flexibility, to build the ability to respond. Now, most of my work is in the private sector, and I have a whole book that talks about how supply chains should build in flexibility so they can respond to all kinds of events regardless of the type of event because the reason for the disruption does not matter. The important thing is that a port is down, a warehouse is down; and when information technology is down, how do you respond to this?

So there are a lot of technical ways to respond to this, and I talk about them in my book. Let me just mention a few that have to do with corporate culture. Because aside from all of the technical and how you build processes, there is an issue of how to build corporate culture, which is based on continuous communication, based on distributing power, decision-making power, to the lowest level in the organization.

It turns out that many organizations where people are passionate about what they do turn out to be very resilient. There is an element of difference to expertise—again, I do not have time to explain it—when you see it in control towers, in chemical plants, in nuclear plants. When something goes wrong, you see that people suddenly do not pay attention to the managers or to the FAA or whatever. They start taking instructions from the veteran people in the tower. They start taking instruction from the gunny sergeant in the foxhole rather than, you know, from the lieutenant.

A good organization, a resilient organization, recognizes it. It allows it. It encourages it. It drills for it.

Finally, let me just say that, you know, drilling, conditioning, conditioning for disruption—I mean, when we are in grade school, and we are told what is the theory of getting out if there is a fire, everybody is instructed to go down. So there is nothing like exercising it, drilling it in terms of getting ready.

Let me stop here, and I will be happy to answer questions later.

Chairman THOMPSON. Thank you very much for your testimony.

[The prepared statement of Mr. Sheffi follows:]

PREPARED STATEMENT OF YOSSI SHEFFI

MAY 6, 2008

RESILIENCE: WHAT IT IS AND HOW TO ACHIEVE IT [1]

My research takes a supply chain perspective on corporate preparedness and response to high-impact/low-probability disruptions. The supply chain of an organization includes the enterprise itself as well as the web of companies and entities that support its operations and service delivery.

The focus of my writings is on resilience—the ability to bounce back from large scale disruptions. In particular, it demonstrates how investments in resilience can be turned into a competitive advantage.

When thinking about the nature of vulnerability and how to build resilience in organizations, one should consider first a framework for defining vulnerability and prioritizing risks. Vulnerability is defined as the combination of disruption likelihood and the resilience of the company to such disruption—whether it can recover

[1] Much more information, including detailed analyses, case studies, numerous examples and recommendations for action are included in my book "The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage" (MIT Press, 2005).

and how quickly. This framework can be used to prioritize all the disruption risks a company faces and thus prioritize the planning for response.

All disruptions can be traced to several generic causes:

- *Random events.* These are natural occurrences such as floods, earthquakes, droughts, etc. Given their frequency, insurance companies can calculate likelihood and create insurance pools.
- *Accidents.* Accidents are typically the result of multiple causes. There is, however, a large body of literature on accident avoidance, based on "near miss" analysis and the "safety pyramid." The experience which this literature is based on includes the aviation, chemical and nuclear industries.
- *Negligence.* Including non-compliance with regulations or standards as well as not paying attention to shifting public attitudes regarding corporate social responsibility.
- *Intentional disruptions.* These include terrorist attacks about also industrial actions, industrial espionage and sabotage. Intentional disruptions are different due the "smart adversary" on the other side; they adapt when defensive measures are put in place.

Compounding effects of large scale disruptions include the following:

- In many cases there is significant public fear (think about SARS, 9/11, Chernobyl)
- Government reaction, which has to come quickly in cases involving public fear, may exacerbate the situation (border closer after 9/11; UK response to the foot and mouth disease, Japanese government reaction to the Kobe earthquake, etc.)
- Living in a connected world, large scale disruptions have cascading effects worldwide
- While the likelihood of individual disaster is small, the likelihood of some disaster taking place somewhere sometime is not insignificant.

The first and most important step in dealing with disruptions is working to avoid them. It is difficult to avoid natural phenomena and there is significant work on avoiding accidents. Avoiding intentional disruptions is the realm of security, however, where one has to focus on the following:

- Layering the defense;
- Balancing the defensive measures;
- Investing in security in accordance with risk ("profiling");
- Collaborating across enterprises, agencies and the citizenry;
- Creating a security culture;
- Practice, practice, practice.

The second step in building resilience is the implementation of a detection system. The most dangerous disruption is the one that is not detected until it is too late. Early detection can trigger early response and, in most cases, a more effective response.

Lastly, the planning and preparation should lay the foundations for a collaborative response. Building joint process, getting to know all organizations involved in a response, assigning specific roles. Of particular importance are public-private partnerships, the utilization of volunteers.

There are basically only two ways to prepare for responding after a disruption hits: building in redundancy and building in flexibility. Redundancy is the first line of defense in case of a disruption. Safety stock of parts and finished goods, spare capacity and multiple suppliers, extra trained personnel, all provide a cushion to absorb some impact. Redundancy, however, is expensive even though there are various forms of minimizing the impact of extra resources and under-utilization. A better strategy is to develop flexibility.

Flexibility has many facets. Consider first, there is the paradox of flexibility: the more standardized many operations and procedures are, the more flexibility they afford. Thus, standard parts, processes, products and procedure, create the ability of their users to be flexible since the users can count on the standards and build on them. Such standardization allows for interchangeability and thus moving resources from where they are to where they are needed in case of a disruption. Just as important, however, is the development of a culture of flexibility. This involves the creation of certain human resources expectations and job definitions as well as cross-training.

The most interesting aspect of building flexibility in an organization is that unlike other resilience measures, flexibility helps companies in the competitive positioning. The reason is that markets around the world are changing at a faster and faster pace. A company that builds in the ability to respond to supply disruption (creating supply/demand imbalance) is automatically building in the ability to respond to demand fluctuations, winning market share.

The important facet of a culture of flexibility and resilience include the following:

- Continuous communications. Resilient companies communicate obsessively so when a disruption takes place people know the exact status of the enterprise. Resilient organizations also have redundant communications capacity, knowing that the volume of communications will grow substantially during a disruption. (Examples: Dell; UPS; counter example: Jet Blue during February 2007)
- Distributed power. Resilient organizations allow every employee, regardless of rank to take decisive action in case of a developing disruption. In the vast majority of the cases, the ability of field personnel to take action quickly can limit the scope of a developing disruption and therefore minimize casualties and damage. (Examples: Toyota's *Andon cord*; U.S. Navy carrier operations; World [Japanese retailer], U.S. Coast Guard operations during Katrina)
- Passion for work and the mission. Resilient organizations demonstrate passionate commitment to the success of their organization, causing employees to go "above and beyond the call of duty." (Examples: Schneider Trucking; Southwest Airlines)
- Deference to expertise. When a disruption is eminent or when it takes place, resilient organizations understand that there is a transfer of deference from rank to expertise (Examples: U.S. Marines, FAA controllers, Chemical plants operators)
- Conditioning for disruptions. Resilient organizations are those that are disrupted continuously. They simply develop expertise at continuous re-planning and getting back to normal operations quickly. (Examples: UPS; FedEx; Counter examples of introducing uncertainty: Intel)

Culture is difficult to define and even more difficult to change. However, there have been spectacular examples of deep culture changes in society and in corporations. These include:

- Safety. During the first part of the 20th century executives used to believe that safety is too expensive to install in plant leading to thousands of casualties in plant and railroad yards. Federal regulations and society's attitude have changed this perception dramatically.
- Quality. The quality of U.S. cars used to embarrass U.S. automotive executives who truly believed that quality is too expansive to install in their cars. Toyota proved the fallacy of this argument and changed the industrial landscape forever.
- Social norms such as smoking as well as drinking and driving have changed dramatically in the United States over the last 20 years.

Thus, corporate and society's culture can change, and senior managers in industry, as well as the Government can have significant influence.

Chairman THOMPSON. I now recognize Chief Southers to summarize his statement for 5 minutes.

STATEMENT OF ERROLL G. SOUTHERS, ASSISTANT CHIEF, HOMELAND SECURITY AND INTELLIGENCE DIVISION, LOS ANGELES WORLD AIRPORTS POLICE DEPARTMENT

Mr. SOUTHERS. Good morning, Mr. Chairman and members of the committee. Thank you very much for inviting me to appear before you this morning to discuss the international, interdisciplinary and risk-based counterterrorism strategies and best practices that we have engaged in at the Los Angeles World Airports.

We placed a high priority on the opportunity to explore and to experiment with possible solutions. For, as my very dear friend and colleague in Israel, Dr. Boaz Ganor, reminds me, at the end of the day, all disciplines are related to terrorism. However, as my colleagues in London, with whom I spent last week at MI–5 and at the New Scotland Yard, will tell you, resiliency is also the capability to detect as well as to recover from disruptive challenges.

This morning, I would like to share with you an innovative framework. Mayor Antonio Villaraigosa has embraced public safety as his No. 1 priority in the city of Los Angeles. During his tenure, crime has fallen to historically low levels. He is a staunch proponent in the area of counterterrorism as well.

He has placed police and counterterrorism professionals in charge of security at the Los Angeles International Airport, an economic anchor for southern California. This resulted in a model consisting of a protective design under the new leadership of the paradigm of the Mayor's appointee, Director James T. Butts, Jr., a former 15-year police chief with 34 years of law enforcement experience.

LAX is safer today than it was 18 months ago. Under their leadership, we have embarked upon a more contemporary and holistic approach to airport policing. This prototype is capable of intelligence analysis, information-sharing, and it facilitates the seamless integration of critical infrastructure protection. We have embraced the mantra of thinking locally and of acting globally.

This year, al Qaeda celebrates its 20th anniversary. A terrorist organization could not exist for two decades without being adaptive, innovative and flexible. The group's capacity to survive is also a direct reflection of both its resilience and the continued resonance of its ideology. However, attackers must conduct surveillance and reconnaissance in order to be successful.

It is a proven fact that randomness increases security. A team of researchers at the Homeland Security Center for Risk and Economic Analysis of Terrorism Events, CREATE, led by Dr. Miland Tambe, work with our department to develop ARMOR, Assistant for Randomized Motoring Over Routes. This software randomizes our vehicle checkpoints along airport access roads and the deployment of our explosives detection K–9 teams throughout the airport.

Peroxide-based explosives represent a new, major, growing challenge to homeland security. We are involved in an international project, researching the properties, detection technology and risk assessment of peroxide-based explosives. This research leverages the combined talents of world renowned Israeli experts at Technion, where Dr. Sheffi is an alum, the Israel Institute of Technology led by Dr. Ehud Keinan, the USC CREATE risk analysts, and our department in order to assess and improve peroxide explosive detection methodology and to optimize deployment strategies for resilience against these attacks.

Last, LAX was selected by DHS to join San Francisco International Airport, SFO, as a pilot site for the chemical, biological, operational technology development, OTD, project. SFO will form the basis for completing a biological response plan, and that plan will be used at LAX. The goal of the LAX chemical OTD restoration project is to develop tools and processes to rapidly restore a critical transportation facility after a chemical agent attack. Upon completion, LAX will be the only airport facility in this country with vetted chemical and biological restoration plans.

A few of our efforts which have aligned the international academic and operational counterterrorism community during the last month include briefing our best practices in Canada, Great Britain, Israel, Jordan, Spain, Thailand, and China. We have assessed the terrorism countermeasures in place for the upcoming 2008 Beijing Olympics. We have our command staff attending the Executive Program in Counterterrorism at USC and at the National Counterterrorism Academy.

For us, war is finite. For terrorists, war is perpetual. Terrorist organizations are becoming increasingly sophisticated at communications and at security awareness. We should learn from failed as well as from successful attacks because, while our vulnerabilities are unlimited, our resources are not. Sustainability is a critical element of resiliency. Also, our intelligence efforts should work on building capacity from the bottom up, local law enforcement.

The progress being made by the Department of Homeland Security at the direction of this committee has been noteworthy. It is an honor and a privilege to be invited to testify and to contribute to the collective national security effort.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions you and the members may have at this time.

Chairman THOMPSON. Thank you for your testimony.

[The prepared statement of Mr. Southers follows:]

PREPARED STATEMENT OF ERROLL G. SOUTHERS

MAY 6, 2008

Chairman Thompson and members of the committee, thank you for inviting me to appear before you this morning to discuss the international, interdisciplinary and risk-based counter-terrorism strategies we are engaged in at the Los Angeles World Airports (LAWA). We have placed a high priority on the opportunity to explore and experiment with possible solutions. As my very dear Israeli colleague and Director of the Institute for Counter-Terrorism in Herzliya Dr. Boaz Ganor, always reminds us, "At the end of the day, all disciplines are related to terrorism!"

I would also like to extend my personal greetings to members Harman, Lundgrun and Sanchez who represent California and often utilize Los Angeles International Airport (LAX). Your leadership in overseeing the Department of Homeland security efforts has paid significant dividends. You and your colleagues have not been afraid to ask the difficult questions and the sense of urgency this committee has brought to homeland security issues has been a catalyst for productive change within homeland security at the Federal, State and local levels.

Resiliency is defined as the capability of a system to maintain its functions and structure in the face of internal and external change. Developing enhanced resiliency is a rational strategy when the probability and specifics of a particular challenge are difficult to define.[1] A resilient society is one that will not disintegrate in the face of adversity. Protecting property and successfully evacuating populations that are potentially in harm's way lessens the destructive impact of a natural disaster. Making infrastructures resilient renders them less attractive targets for terrorists. Preparing for the worst makes the worst less likely to happen.[2] We cannot stop every terrorist attack. We can however, reduce the risk and enhance the capability for our continuity of operations.

This morning, I would like to share an innovative framework with you. Mayor Antonio Villaraigosa has embraced public safety as his No. 1 priority in the city of Los Angeles. During his tenure, crime has fallen to historically low levels. He is a staunch proponent in the area of counter terrorism as well. He has placed police and counter terrorism professionals in charge of security at Los Angeles International Airport, an economic anchor for southern California. This resulted in a model consisting of a protective design under the new leadership paradigm of the Mayor's appointee, Director James T. Butts, Jr., a former 15-year police chief and 34-year law enforcement professional. LAX today is safer than it was just 18 months ago. Under their leadership, we have embarked upon a more contemporary and holistic approach to airport policing. This prototype is capable of intelligence analysis, information sharing and facilitates the seamless integration of critical infrastructure protection. He has created an organizational structure and a counter-terrorism element unprecedented in the airport environment. By harnessing our strengths and

[1] Allenby, Brad and Jonathan Fink. *Toward Inherently Secure and Resilient Societies.* Science Magazine, August 12, 2005.

[2] Flynn, Stephen. *The Edge of Disaster.* Random House, New York. (2007) p. 154.

leveraging our relationships, we have transformed the No. 1 airport terrorist target in the Nation into an operational think-tank, capable of placing theory into practice and creating a dynamic response to the transnational threat of terrorism. We have embraced the mantra of "thinking locally and acting globally."

INTRODUCTION

Los Angeles International Airport is the world's busiest origin and destination (O&D) airport, meaning O&D passengers are those beginning or ending their trips in Southern California rather than using the airport for connecting flights. In total traffic, LAX is the fifth busiest airport in the world for passengers and ranks 11th in the world in air cargo tonnage handled. In 2007, the airlines of LAX served 61.9 million passengers and handled 2 million tons of freight and mail. LAX handled 70 percent of the passengers, 75 percent of the air cargo, and 95 percent of the international passengers and cargo traffic in the five-county Southern California region.

LAX also creates jobs. An estimated 59,000 jobs, directly attributable to LAX, are located on or near the airport. Approximately 408,000 jobs, spread throughout the region, are attributable to LAX. The employment in the city of Los Angeles due to the airport is estimated to be 158,000 jobs. One in 20 jobs in Southern California is attributed to LAX operations.

In fiscal terms, LAX is a dynamic airport which creates, attracts and supports economic activity throughout Southern California. International flights arriving at LAX from overseas make a substantial contribution to the economy of Southern California, adding $82.1 billion in total economic output, plus 363,700 direct and indirect jobs with annual wages of $19.3 billion in Los Angeles, Orange, Riverside, San Bernardino, San Diego and Ventura Counties, according to a 2007 study by the Los Angeles Economic Development Corporation. Unfortunately, this fiscal vitality also bodes well in terms of its attractiveness as a terrorist target.

HISTORY

Terrorism has long been a serious threat to the air transportation system of the United States and other nations. "Over 5,000 deaths have resulted from terrorist attacks on civil aviation since 1980; about 200 deaths occurred in attacks on airports themselves, as opposed to aircraft."[3] Apart from the major changes in the Nation's defense posture, we know that the economic effects of the September 11, 2001 terrorist attacks were relatively short-term in their impact. Thus, in one of the first studies undertaken at the Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE), we considered the short-term economic costs of an attack on the U.S. commercial air system.

We modeled a 7-day shut-down of the entire U.S. commercial air transportation system, followed by a 2-year period of recovery, using the post-September 11 experience of the system as a basis for our analysis. Our overall loss estimates for the 2 years range from $248 to $394 billion.[4]

In another study of this catastrophic attack, the results concluded the following losses:

- First day Wall Street losses: 16 percent
- Gross amount traded per day: $4 trillion
- Total loss from stocks = $640 billion
- American daily income = $20 billion
- First week loss = $140 billion
- Total national loss = $780 billion
- Building & Construction losses = $30 billion
- Liquidated 170,000 employees from airline companies
- American studies estimated 70 percent American people suffering from depression
- Intercontinental Hotel—20,000 job losses

One would assume the researchers in this study represented a think tank or major research university. In fact, these figures were the results of an economic analysis articulated by Osama bin Laden, in his October 21, 2001 interview with Taysir Alluni, head of al-Jazeera's bureau in Kabul.[5] Regardless of the mathe-

[3] See the Memorial Institute for the Prevention of Terrorism (MIPT) Knowledge Base, online at *http://www.tkb.org.*

[4] Gordon, Peter. *The Economic Impacts of a Terrorist Attack on the U.S. Commercial Aviation System.* Center for Risk and Economic Analysis of Terrorism Events (CREATE) Report No. 05–026. (2005)

[5] Lawrence, Bruce. *Messages To The World, The Statements of Osama bin Laden.* Verso, London and New York. (2005) pp. 111–112.

matical accuracy of al Qaeda's study, they clearly appreciate the value of an attack beyond the loss of life.

Interestingly, LAX has been described by RAND as "a leader in implementing new security measures."[6] It was one of the first major airports to implement a 100 percent baggage-screening program, a dedicated and high visibility police department, onsite bomb squad, the largest number of explosives detection canine teams at an airport in the world and a dispersed central terminal design. Despite this level of protection, LAX is viewed as an attractive target by some terrorist organizations having been targeted six (6) times—more than any other airport in the world!

Since 1974, LAX has been the target of two bombings, two attempted bombings, one gun attack and one combination bombing/active shooter attack. In 1974, "Alphabet Bomber" Muharem Kurbegovic detonated a bomb in the LAX international terminal, killing three and injuring eight. A bomb exploded in 1980, in the China Airlines luggage processing facility, causing extensive damage but no injuries. In May 1982, three members of the Armenian Secret Army for the Liberation of Armenia were arrested after placing a bomb at the Air Canada cargo office.

Ahmed Ressam was caught crossing into the United States in 1999, with bomb-making equipment. His plan, later known as "The Millennium Plot," was to detonate four timed luggage bombs inside and curbside at the Tom Bradley International Terminal (TBIT). My colleague and CNN terrorism analyst Peter Bergen, best known for his interview of Osama bin Laden believes, "The millennium plotting in Canada in 1999 may have been part of Bin Laden's first serious attempt to implement a terrorist strike in the United States." Ressam has told the FBI that he conceived the idea to attack Los Angeles International Airport himself, but that bin Laden lieutenant Abu Zubaydah encouraged him and helped facilitate the operation.[7]

On July 4, 2002, Hesham Hadayet approached the El Al counter with two handguns, killing two and injuring six. In 2005, a radicalized al Qaeda based group formed in Folsom Prison, plotted to again attack the El Al ticket counter, in addition to the Israeli Consulate, two National Guard recruiting centers and several synagogues in simultaneous bombings and active shooter operations across Los Angeles. When the suspects were convicted, it was learned they admitted to being 2 weeks away from executing the attacks. LAX remains a very attractive target.

I have had the opportunity to visit and review the protective measures with my colleagues at several airports considered to be target-rich including; Ben Gurion in Israel, considered to be one of the world's most secure, Heathrow in Great Britain, the world's busiest airport and which recently opened a state-of-the-art terminal and Beijing International in China, which recently opened the world's largest terminal and will host the 2008 Olympic Games. We all agree on three basic realities—reducing the risk of terrorism and public safety is paramount, emergency response efficiency is critical and the continuity of operations subsequent to a natural or man-enabled event will have severe impact on the global economy.

LOS ANGELES WORLD AIRPORTS POLICE ORGANIZATIONAL RESPONSE

As Congresswoman Harman is uniquely aware, RAND Corporation was commissioned by Los Angeles World Airports to conduct a series of studies on options for protecting the airport from terrorism. RAND identified 11 major scenarios of attacks in the following ascending order: mortar attack, sniper attack, control tower bomb, MANPADS attack, air operations attack, public ground attack, curbside bomb attack, luggage bomb, large truck bomb, uninspected cargo bomb and insider planted bomb. The top 5 scenarios involve explosive devices, vehicle and/or employee access. The subsequent re-organization of our department is in direct response to the study. The Homeland Security and Intelligence Division is comprised of the Critical Infrastructure Protection Unit, Vulnerability Assessment and Analysis Unit, Emergency Services Unit, Dignitary Protection Unit, Canine Unit and the Security Credential Unit.

This reorganization facilitates the effective response to the 5 "major" terror scenarios by reducing bureaucracy, increasing unit responsibility and ensuring management accountability. For example, the Security Credential Section is responsible for the processing, vetting and management of more than 40,000 LAX badge holders, more than 52,000 for the Los Angeles World Airports, including Palmdale, On-

---

[6] Stevens, Donald, Thomas Hamilton, Marvin Schaffer, Diana Dunham-Scott, Jamison Jo Medby, Edward W. Chan, John Gibson, Mel Eisman, Richard Mesic, Charles T. Kelley, Jr., Julie Kim, Tom LaTourrette, K. Jack Riley, *Implementing Security Improvement Options at Los Angeles International Airport,* Santa Monica, California: RAND Corporation, 2006.

[7] Bergen, Peter L., *The Osama bin Laden I Know.* Free Press, New York, NY (2006) pp. 289–290.

tario and Van Nuys airport which happens to be the busiest general aviation airport in the nation. The new centralization of the badging process also lends itself to easy information sharing and analysis as it relates to our properties. In the midst of a recent event one morning when we thought an individual had boarded an outbound flight posing as an employee, it was the information from the Security Credential Unit that proved most valuable in the suspect elimination process before the diverted flight had even landed.

In addition to the RAND study, we are routinely evaluated in a joint assessment by the TSA and FBI to determine our Man Portable Aerial Defense (MANPAD) vulnerabilities. We have also invited our colleagues from Ben Gurion Airport to evaluate our protective measures. Guided by the three studies we maintain a Critical Infrastructure Protection Unit and a Vulnerability Assessment and Analysis Unit, charged with meeting the goals of Homeland Security Presidential Directive-7, the identification, protection and prioritization of critical infrastructure and ensuring TSA Security Directive compliance respectively. These units also work in concert with our local, State and Federal regulatory airport partners monthly, as the Cargo Security Task Force, descending unannounced on cargo facilities to evaluate all personnel, security and safety related compliance issues.

TERRORIST OPERATIONAL PLANNING CYCLE

This year, al Qaeda celebrates its 20th anniversary. A terrorist organization could not survive for 2 decades without being adaptive, innovative and flexible. In fact, every attack in the last 4 years in Europe (except the Van Gogh murder) has had al Qaeda connectivity. Commercial aviation is the most institutionally hardened critical infrastructure since the attacks on September 11, yet it remains the most desirable target. Al Qaeda's global network has endured by its members strictly adhering to the principles of operational security.

In addition to the al Qaeda threat, the death of Imad Mughniyah, by a bomb blast on February 12, 2008, has heightened our concerns regarding the threat of attack by Hezbollah. Mughniyah, a senior member of Hezbollah, was associated with the Beirut barracks and United States Embassy bombings in 1983, which killed over 350, as well as the kidnapping of dozens of foreigners in Lebanon in the 1980's. He was indicted in Argentina for his role in the 1992 Israeli Embassy attack in Buenos Aires.

In response to this specific threat and the fact that El Al has been targeted 3 times since the new millennium, our Emergency Services Unit (ESU) provides special weapons and tactics security for El Al passengers during ticketing/check-in, escorts their busses to the terminal and remains on the airfield until the aircraft departs. In addition to their already unique skillset, all members of our ESU have completed the DHS Prevention & Response to Suicide Bombing Incidents Training Course. El Al has informed us LAX is the only airport outside of Israel that affords them this level of security.

Terrorist groups, particularly al Qaeda, conduct surveillance and reconnaissance to select potential targets to gain strong situational awareness of the target's activities, design, facility vulnerabilities and security operations. Because part of the preoperational surveillance involves establishing patterns, terrorists will conduct their surveillance multiple times. However, the more they conduct surveillance, the greater the chances of being observed themselves. If they are observed, their entire plan can be compromised by alerting security personnel to the fact that something is being planned.

Al Qaeda training manuals, including the infamous "Military Studies in the Jihad Against the Tyrants," and their online training magazines instruct operatives to perform surveillance, and even go so far as to discuss what type of information to gather. In July 2004, the arrest in Pakistan of an individual identified by U.S. officials as Mohammad Naeem Noor Khan revealed a personal computer that contained detailed information about potential economic targets in the United States. The targets included the New York Stock Exchange and Citigroup headquarters in New York, the International Monetary Fund and World Bank buildings in Washington, DC, and Prudential Financial headquarters in Newark, NJ. From the information on the computer, it appeared that the targets were under surveillance for an extended period.

In the case of the aforementioned pre-attack planning cycle, there was a high degree of detail and awareness of site vulnerabilities, security operations and law enforcement and emergency response at the time the reports were written. In addition to intelligence obtained from surveillance, each of the surveillance reports exhibited extensive use of open-sources to obtain much of the background information on the target. It should be noted the report provided alternative targets should attacking

the primary site prove to be logistically unfeasible. The focus on collecting data on alternate, less protected locations indicates al Qaeda's interest in softer targets. This may be reflective of al Qaeda's evolution from a centrally directed organization into a more decentralized structure possessing greater control over target selection.

Surveillance can occur in as little as 1 week, to as long as several years prior to an attack and can be used to support target selection, mid-operation reconnaissance and final, pre-attack reconnaissance. Surveillance is typically conducted in a covert manner and can involve any number of collectors (surveillants) either on foot or in vehicles. Successful counter-surveillance can yield indications of an attack planning phase. The problem is separating "terrorism" from "tourism." Herein lies the importance of employing a strategy that facilitates "looking for the bombers and not the bombs."

AUTOMATED LICENSE PLATE RECOGNITION TECHNOLOGY

Actionable intelligence, accompanied by education, awareness and technology are essential resources to be effective in these efforts. A debrief of the attack on the Kohbar Towers bombing, determined the target was surveilled more than 40 times over a 17-month period, by the same three attackers. On at least 10 of those reconnaissance missions, the attackers visited the site in the same vehicle.

The fact that more than 50,000 vehicles enter LAX daily, makes vehicle surveillance a simple task, utilizing Automated License Plate Recognition (ALPR) technology. This is a proven method that automatically identifies license plate numbers on stationary or moving vehicles (at speeds of over 140 mph), captures images of the vehicle license plate and instantly checks those numbers against a data base. Every license plate scanned is compared to a list of "vehicles of interest" associated with auto theft, felony warrants, Amber Alerts, DOJ & NCIC downloads, parking violations, or any other license plate-oriented databases. Our anticipated acquisition and implementation of this technology will essentially limit the capacity of attackers to use the roadways!

The database can be designed to be triggered if the license plate entered the area based on frequency, time of day, day of the week, etc. Inasmuch as repeated trips are necessary for terrorists to obtain the desired situational awareness, this would be a useful countermeasure. Ben Gurion Airport has deployed this system on its main access road, in a toll-booth design, to capture the license plate of every vehicle entering the central terminal area. The system is also in use in Europe in Birmingham, Edinburgh and Glasgow Airports.

A recent case suggests that given access to this technology, valuable investigative time could be significantly reduced. A rent-a-car manager at an airport reported activity he found to be suspicious. The manager stated that during an 11-month period, four adult males of Middle Eastern ancestry rented vehicles numerous times and each time the vehicles were returned with excessively high mileage. An example provided revealed a vehicle had been rented for 10 days. The vehicle had been driven 3,848 miles during the rental period, which is considered excessive by rental car standards. Additionally, numerous employees of the rental car agency observed shopping bags containing new wrapped pre-paid cell phones in the vehicle, which were taken by the subjects with the rest of their personal property when they returned the rental vehicle.

In this instance, if ALPR were deployed, we would know if the vehicle accessed our airport, the frequency of those "visits," and the exact dates. Accompanied by the other available technology systems, we could organize and analyze vast quantities of structured and seemingly unrelated data, currently housed in various incompatible databases and record management systems, over a highly secure intranet-based platform. Inasmuch as we contact and complete field interview cards, crime reports and obtain information from individuals from all over the world on a daily basis, makes LAX an incredible source of information.

CREATE RANDOMIZATION PROJECT

The Center for Risk and Economic Analysis of Terrorism Events (CREATE) is an interdisciplinary national research center based at the University of Southern California and funded by the Department of Homeland Security. The Center is focused on risk and economic analysis of the U.S. infrastructure and comprises a team of experts from several universities from across the country. It was the first of 13 existing Centers of Excellence in the Nation and the only Center whose grant has been renewed thus far.

As previously described, the al-Qaeda planning cycle, depends on the comprehensive situational awareness acquired via pre-attack surveillance and reconnaissance of the intended target. It is most important for the attackers to determine the de-

sign and level of physical security, including protective policies, procedures and technology. A team of researchers at CREATE led by Dr. Miland Tambe, working with our department developed software that would offer assistance regarding the deployment of critical terrorism countermeasures. Dr. Tambe's expertise is in the area of Security in Multiagent Systems by Policy Randomization.

It is a proven fact randomness increases security. Randomization methodology was theoretically proposed by CREATE to assist in the deployment strategy of unmanned aerial vehicle (UAV) flights over Afghanistan. The goal of our project was to leverage CREATE's success by randomizing vehicle checkpoints being deployed along airport access roads.

The program, based on Bayesian Stackelberg game theory, was developed to allow for the input of certain constraints regarding the checkpoint, the avoidance of certain days for deployment and the necessity for the checkpoint to be in effect during specific times during the day. Based on these constraints, the program provided a randomized schedule, in conjunction with a mathematical measure of randomness. Additional features are added to the program to facilitate the input of the constraints and create a report at the end of a checkpoint in operation.

Such scheduling is based on several requirements:

(a) Scheduling must be randomized to avoid predictability;

(b) Scheduling must take into account constraints of officers at LAX;

(c) Scheduling must take into account passenger load data;

(d) Scheduling must also take into account other possible resource constraints, dynamic shifts and so on.

The USC CREATE team attacked this scheduling problem in a multi-phased approach. The first phase focused on scheduling checkpoints, and in particular using the first two criteria mentioned above. The next step in the project incorporated the explosives detection canine team deployment into the program development. Inasmuch as LAWA maintains 32 explosives detection canine teams, this asset renders LAX the perfect environment for this research. Upon completion, we anticipate leveraging the program for the purpose of randomizing the deployment of patrol, bicycle officers and other Airport Police resources.

After several months of operation and in accordance with the National Infrastructure Protection Plan Risk Management Framework, we decided to develop an evaluation feedback loop consisting of graduate students, who unbeknownst to them, were challenged with testing the resiliency of the system. They played a game called "Pirates and Treasures." The students were instructed to identify ways to breach the security of the system and were rewarded with points during the course of the game. These results were analyzed and provided the basis for a revision of the game theory algorithm inherent in ARMOR software.

The results of this premier engagement in "Translational Research," that is research which translates directly from the laboratory to the field and the practitioner, could not have been anticipated. We have received inquiries from a host of Federal agencies and countries as far away as India. We briefed the Transportation Security Administration last year in anticipation of the program being utilized to randomize the deployment of Federal Air Marshals on flights. Praveen Pachuri, the doctoral student who developed the algorithm, is being actively sought by a host of defense contractors as a result of the programs' success.

PEROXIDE-BASED EXPLOSIVES RESEARCH PROJECT

Peroxide based explosives, including TATP (triacetonetriperoxide), DADP (diacetonediperoxide) and HMTD (hexamethylenetriperoxide-diamine), represent a major, growing challenge to homeland security. The threat has been recently highlighted by a number of terrorist events worldwide, such as the 2005 attack on the London public transportation system, the intercepted 2006 terrorist plot to target airliners en route from London to the United States, and many car and suicide bombings in the Middle East.

The Los Angeles World Airports Police Department is involved in an international project researching the "properties, detection technology and risk assessment" of peroxide-based explosives. The research leverages the combined talents of world-renowned Israeli explosives experts at Technion—Israel Institute of Technology, led by Dr. Ehud Keinan, USC CREATE risk analysts, led by Drs. Isaac Maya and Onur Bakir, and Los Angeles World Airports Police Department personnel in order to assess and improve peroxide explosive detection methodologies and optimize deployment strategies for those technologies.

The United States has already experienced its first suicide bomber. In 2005, Joel Hinrichs, III, an Engineering graduate student at the University of Oklahoma, blew himself up outside of the school's Memorial Stadium. He was denied entry because

he would not allow security personnel to examine the contents of his backpack which contained a TATP improvised explosive device, before entering the stadium with 84,000 people in attendance.

Doubt was cast subsequent to this incident with regards to Mr. Hinrichs' intent or social network. Investigation reveals he constructed the bomb via an Internet recipe after he unsuccessfully attempted to purchase ammonium nitrate. Going to the football game should certainly demonstrate his intent, the fact that he attended a Mosque in Norman, Oklahoma visited by Zacarias Moussaoui, and September 11 hijackers, Marwan Al-Shehhi and Mohammed Atta, would suggest indirect, if not direct connectivity to an environment with some very dangerous people.

Altogether, TATP, HMTD and other peroxide-based explosives pose a multifaceted, intricate challenge to public security. As their density (0.5 g/mL) is similar to that of most common organic solids, such as white sugar, it is not possible to detect them by the CTX machines that are currently deployed in airports for the detection of conventional explosives. Although the most urgent need is the development of detection and identification methods, there are many other aspects of the problem that should be pursued. These include fast and reliable onsite neutralization of captured materials, comprehensive study of their chemistry and properties, including post-blast analysis and identification of the type, quality, manufacturing methods, as well as the origin of captured improvised explosive devices.

The goals of the research project are articulated as follows:

(a) Preparing a broad variety of plastic TATP explosives in order to develop recommendations regarding their detection, characterization and safe handling.

(b) Identify and characterize the various polymorphic crystals of TATP and develop reliable detection methodology utilizing XRD technology.

(c) Using formal risk assessment methodologies to analyze the comparative costs and benefits of deploying peroxide-based explosive detection technologies at the Los Angeles International Airport and therefore, possibly other major transportation infrastructures engaged in passenger screening operations.

CHEMICAL OPERATIONAL TECHNOLOGY DEVELOPMENT RESTORATION PROJECT

LAX was selected by DHS to join San Francisco International Airport (SFO) as a pilot site for the Chemical/Biological Operational Technology Development (OTD) Project. SFO has been the primary partner airport for developing plans for Biological Incidents. Once that plan is developed it will be the basis for the completion of a Biological Restoration Plan for LAX. The goal of the LAX Chemical OTD Restoration Project is to develop tools and processes to rapidly restore a critical transportation facility after a chemical warfare agent attack. Upon completion, LAX will be the only airport facility with vetted chemical and biological restoration plans.

AIRPORT POLICE STRATEGIES AND INITIATIVES

The Los Angeles World Airports Police initiatives have aligned the international academic and operational counter-terrorism community. We are part of a global network capable of identifying and disrupting the ability of attackers' efforts to recruit, fund, plan, surveil or execute terror operations. Our efforts to date include:

- During this past year, our officers have studied and/or delivered counter-terrorism briefs in Canada, Great Britain, Israel, Jordan, Spain, Thailand, and China.
- Airport Police hosts a bi-weekly Community Awareness Meeting with area business owners, community groups and residents for the purpose of sharing information related to crime activity, law enforcement projects and other relevant airport information available to us from our partners across the Nation.
- Airport Police detectives are assigned to the Joint Terrorism Task Force and the Joint Regional Intelligence Center.
- Our Canine Unit Officer-in-Charge was appointed the International Liaison for the Detector Dogs World Congress regarding all explosives detection canine matters.
- We accepted an invitation to travel to Beijing, Shanghai and Qingdao for the purpose of assessing the terrorism countermeasures in place for the XXIX Olympiad.
- Officers are enrolled in the Executive Program in Counter-Terrorism at USC and the Manhattan Institute National Counter-Terrorism Academy.
- During terminal evacuations related to the detection of "possible improvised explosive devices" (IEDs) identified at screening stations, announcements to passengers articulate the reason for the evacuation, efforts are made to provide a comfortable environment, with seating and water if possible and seniors and

parents with children are given priority for re-entry into the terminal after the incident is resolved.
- Airport police work in concert with the bomb squad and TSA on every terminal IED-related evacuation to minimize the impact to vehicular traffic in the central terminal area and expedite the repopulation of the screening stations. All of these events are timed and de-briefed.

During my tenure as Deputy Director in the Governor's Office of Homeland Security, the resiliency of the Port of Los Angeles-Long Beach and LAX were regular topics of discussion. In response to the 9/11 Commissions overall critique of our inadequate intelligence sharing capabilities; the ports created the Area Maritime Security Committee (AMSC). The AMSC consists of local, State and Federal intelligence professionals and first responders for the purpose of identifying vulnerabilities, determining possible risk-reduction strategies and engaging in training and exercises during scenarios to protect the maritime environment.

As a result of the success of the AMSC, we transplanted the group to LAX in an effort to mirror the strategy with most of the same entities charged with responding to the threat at the ports. Director Butts co-chairs the Airport Security Advisory Committee, which has benefited from existing professional relationships, thus creating an institutional knowledge with expertise and experience focused on the protection of two extremely vital sites, other critical infrastructure in the region and the global importance incumbent upon their resiliency.

LAWA SECURITY TECHNOLOGY INITIATIVE

In 2006, we initiated a comprehensive analysis of the three separate airport infrastructure vulnerability studies—RAND, TSA-FBI MANPADS Mitigation Report and the Ben Gurion Assessment. These evaluations not only examined security gaps, they recommended the most efficient and cost-effective solutions to enhancing security measures within the Los Angeles World Airport system. To that end the Security Technology Initiative is the technology infrastructure backbone that would integrate our current and long-term counter-terrorism efforts. We have hardened our security infrastructure and seek to improve our situational awareness through the implementation of advanced technology such as ALPR, smart video analytics, and perimeter intrusion detection systems.

CLOSING

For us, war is finite, for the terrorist war is perpetual. Osama bin Laden has identified a timeline of 1,400 years to accomplish his mission. In the meantime, terrorist organizations are becoming increasingly sophisticated in communications and security awareness. As an example, terrorists are leveraging terror trials and court testimony as an additional opportunity to identify our counter-terrorism investigative methodologies.

Our intelligence efforts should work on building capacity from the bottom up—local law enforcement. Our success in deterring terrorist attacks rests with our ability to make the environment more difficult for attackers to operate. Timothy McVeigh, Eric Rudolph and the JIS group spawned in Folsom Prison were arrested as a result of good police work.

Commercial aviation is the most institutionally hardened critical infrastructure since 9/11. Yet, last summer it was targeted again. We should learn from failed, as well as successful attacks because, while our vulnerabilities are unlimited, our resources are not. Sustainability is a critical element of resiliency.

The need for the continuing support for the collaborative efforts of the Department of Homeland Security's Science and Technology Directorate and its Centers of Excellence is critical. We must facilitate the link between the laboratory and the operational world. Our best-practices clearly illustrate the potential when these relationships are realized.

The progress being made by the Department of Homeland Security at the direction of this committee has been noteworthy. It is an honor and a privilege to be invited to testify and to contribute to the collective national security effort.

Chairman THOMPSON. I now recognize Dr. Bailey to summarize her statement for 5 minutes.

STATEMENT OF SUSAN R. BAILEY, PH.D., VICE PRESIDENT, GLOBAL NETWORK OPERATIONS PLANNING, AT&T INC.

Ms. BAILEY. Thank you, Mr. Chairman, Ranking Member King and members of the committee.

My name is Dr. Susan Bailey, and I am AT&T's Vice President for Global Network Operations Planning. In that role, I am responsible for designing AT&T's unified network operations model, which includes our network's business continuity and disaster recovery. In addition, I have direct operational experience in addressing some of the worst national disasters in recent years.

As the Nation's largest communications company and as a major global carrier, AT&T is a critical link in keeping our society connected, especially during disasters. We recognize that within our footprint we provide lifeline and emergency communications services for the communities and people in our footprint. In addition, we also recognize that on our infrastructure, key government agencies and all of the major critical infrastructures in our economy provide or use our infrastructure for carrying their mission-critical applications and communications services, so we recognize firsthand that people's lives and safety, as well as the very function of our government and of our economy, depend on AT&T's ability to maintain our network infrastructure and on the services we provide.

We take this responsibility very seriously, and we approach disaster preparedness as a fundamental operational requirement that we architect into the core of our network and in how we approach our operations.

Now, AT&T focuses our business continuity approach on functional resiliency as distinguished from asset protection. We certainly do take action to protect our assets, but the notion of functional resiliency is that our mission-critical functions can carry forward and can be sustained despite the loss of individual assets. So we design our network, our work centers and the operational processes within them, as well as our support systems and our information technology, with backup plans and with alternate arrangements so that we can sustain those mission-critical applications and operations despite the loss of individual assets.

Now, since it is very seasonal that the 2008 hurricane season is fast approaching, right around the corner, I thought I would say a few words about some of the things that AT&T is doing to prepare for the upcoming hurricane season.

Now, since the hurricane season tends to impact the Southeast United States more significantly than other parts of the country, we have actually looked at our traffic volumes. Based on predictions of increased volumes on our wireless network, we have taken action to expand our capacity to be prepared for, you know, the increased load that we would project in a disaster scenario.

In addition, hurricanes are largely power events for us where, you know, we lose commercial power and need to sustain our network despite the loss of commercial power. So we put a lot of energy up front into validating the readiness of our power and infrastructure with respect to having extended-life batteries, in topping off our fuel tanks, in testing our generators, and in deploying more generators both on a permanent basis as well as mobile generators that we can move around to our locations as we need to.

In some cases, we have actually installed permanent generators that run on natural gas, which frees us up from the need of having to refuel those generators.

Now, we maintain a large fleet of mobile disaster recovery trailers, that are basically central offices on wheels, along with emergency communication vehicles, mobile command centers, HAZMAT equipment, decontamination trailers. We look at the profile of where we have got that equipment as it is located in warehouses around the country and around the world, and we will actually preplan and will dispatch additional equipment toward the Southeast so it is ready to be deployed on short notice.

Now, in the area of cybersecurity, AT&T has unique capabilities on both the prediction and the prevention, as well as on the mitigation and response. On the predictive side, we have the ability to pattern and to profile our network traffic on our Internet backbone, based on time of day, day of week and types of traffic from point to point. When we know what "normal" looks like, we have the ability to take abnormalities such as hackers who are testing out their malicious code or who are probing the network, looking for vulnerabilities; and we use that ability to detect abnormalities, to give us that advanced alert, so that we can take action in advance to protect our network before the actual launch of a cyber attack.

Now, on the mitigation and response side, we offer our customers a distributed denial of service remediation. A distributed denial of service attack is basically lots of traffic headed toward a particular machine or a particular Internet IP address that consumes that machine with having to respond to lots of brief inquiries. We have the ability from the core of our network to redirect traffic toward scrubbers that are imbedded within our network, and those scrubbers can then, based on the signature of the malicious attack traffic, filter out the bad traffic and then reinsert the good traffic back toward its ultimate destination.

Thank you very much, and I am looking forward to entertaining questions.

Chairman THOMPSON. Thank you for your testimony.

[The prepared statement of Ms. Bailey follows:]

PREPARED STATEMENT OF SUSAN R. BAILEY

MAY 6, 2008

My name is Dr. Susan R. Bailey. I am AT&T's Vice President, Global Network Operations Planning, located in Bedminster, New Jersey. I appreciate the opportunity to share ideas with Members of Congress and other industry participants to enhance America's homeland security capabilities.

I have over 20 years of experience in developing, deploying and operating advanced communications technologies and support systems, and have held numerous positions in planning, network operations, and product research and development. In my current role, I develop the network operations model spanning all services and technologies for the entire company, including global and long distance services, regional access, wireless mobility, and video applications. I am, therefore, intimately familiar with AT&T's principles and methods for building and maintaining a robust communications infrastructure.

As the Nation's largest communications company, AT&T is a critical link in keeping our society connected—especially during disasters. Among other things, we provide lifeline and emergency communications to millions of consumers and businesses; mission-critical support for government agencies and institutions; and robust communications networks and support for the full range of business enterprises, including in the healthcare, electric power and banking sectors. We know that, in many ways, peoples' lives and safety, as well as the function of our government and economy, depend on the services we provide. For these reasons, ensuring that our component of the Nation's infrastructure is sound and resilient is one of our top priorities.

The following outlines AT&T's approach to protecting its network and responding to disasters, and includes some examples of that approach in action.

AT&T'S NETWORK REACH

AT&T operates one of the most extensive communications networks on the planet. We have deployed and maintain more than 500,000 miles of fiber in the United States, under the oceans, and around the world. Every day our network carries more than 16 petabytes of data—the equivalent of moving the entire written contents of the Library of Congress every 35 seconds. In the United States, we are the leading provider of broadband Internet access services; the leading wireless provider—able to offer 3G wireless broadband in 265 major metropolitan areas; and the leading provider of telephone service in rural areas. We have equipment deployed to serve 143 countries. All told, over 1 billion devices are connected to AT&T's network, and we make data services available to 97% of the world economy.

The breadth of AT&T's network allows us to provide unmatched quality across an unmatched range of services, but it also necessarily means that our capabilities are subject to a wide range of threats. These threats include power outages, hurricanes, typhoons, earthquakes, terrorist attacks, and even an otherwise innocuous fiber-seeking backhoe that accidentally strikes an underground cable. Moreover, we see indications of nearly 39 million potential cyber-attacks every month; while these do not result in physical damage, they can wreak havoc on the logic of a network that is not adequately defended. And, of course, health pandemics, transit disruptions, or work stoppages can affect our workforce, which in turn can directly impact our networks. We worry about and plan for all these incidents—and more.

AT&T'S APPROACH TO BUSINESS CONTINUITY AND NETWORK RESILIENCY

AT&T is in the business of connecting people anywhere and any time. In order to connect people, continuity of operations is critical. The hallmark of our business continuity program is a common, structured approach to infrastructure design, management, and execution.

Our enterprise business continuity paradigm focuses on protecting three types of assets:

(1) The network itself, i.e., the computers, switches, routers and fibers that carry our customers' data.

(2) Work centers and the people who work in them, in particular those that perform mission-critical help-desk and network operations functions. We plan for the safe evacuation of our people through emergency communications and evacuation plans. And we plan for the recovery of mission-critical work functions, such as customer help desk and network operations, in alternate locations or arrangements.

(3) Network management tools, such as network and customer databases, ticketing systems, provisioning and alarm management systems, and business process automation platforms.

More specifically, AT&T focuses on service or functional resiliency. At its core, this means the continued operation of a function despite the loss of certain assets and controlling the impact once a threat arises. This compares to a strategy that unduly emphasizes the elimination of all possible threats. We cannot prevent a tornado or earthquake—or a terrorist attack—from destroying one of our buildings. But we can protect the functions performed in that location, such as by maintaining an alternate site geographically distanced from the primary site. To be clear, we certainly do our fair share of asset protection, such as securing the physical environment along our fiber routes or employing building security. But no amount of protection can possibly guarantee that any asset can completely be protected.

AT&T'S PHILOSOPHY IN ACTION

Consistent with our general philosophy, we leverage technology to protect functions and the services despite failure and disasters. For example, the telecommunications infrastructure depends heavily on commercial power. We therefore build resiliency into our major offices by connecting them to two different and diverse electrical substations. In addition, we equip them with battery backup and auto-start generators for continuous operation in the absence of commercial power. This funda-

mental design has sustained us through even widespread power outages, such as the widespread power outage of 2003.[1]

In addition to diversity of power, we employ diversity of fiber and other equipment. For example, most of our fiber routes have a physically diverse, geographically separated alternate route. This physical fiber diversity extends all the way to building entrances. In addition, the fiber connections to our major central offices have two separate entrances at different places within the building. Likewise, customer applications or data storage solutions can be hosted in any of AT&T's 38 worldwide internet data centers, with backup and failover capacity to provide uninterrupted capability even in the face of the loss of an entire data center. Servers and databases for a given application can be deployed, for instance, in a data center on the west coast and another on the east coast, perhaps configured to share the load between them under normal operating conditions. If, for whatever reason, one of the centers fails, the other could pick up the load and continue with uninterrupted service.

One of our most powerful assets to handle disasters of almost any kind is our fleet of more than 500 trailers equipped with all the gear we need to run our network—routers, switches, multiplexers and the like; these are mobile central offices. AT&T has been building and expanding this fleet for more than 15 years and so far has invested over $500 million in these disaster recovery assets. On a normal day, the trailers are stored in warehouses around the world. But they are not just collecting dust: they are right now connected to our network, monitored and managed, upgraded and repaired, just like any other element of our network. If we need any of the equipment, we can literally unplug a trailer, hook it up to a truck, and drive it to wherever we need it. And, we have software support that enables us to download all of the configurations that we use throughout our system almost instantly, which reduces the actual turn-up time at a site down to our objective of 72 hours. We test our disaster response capability four times per year so that we are ready to respond. In fact, at the same time as this hearing, AT&T will be conducting a simulated disaster scenario in Chicago.

Perhaps the most storied use of our mobile network facilities was in connection with the horrific events of 9/11. Because our mobile equipment is capable of operating in the stead of even the largest of our major central offices, we were able to use them to recover our transport hub that was in the 6th sub-basement of the World Trade Center South Tower, which was totally destroyed, as well as support three switches in nearby buildings that were heavily damaged. We dispatched trailers to New York, and by noon that day they were setting up in a parking lot across the river in Jersey City. Within 48 hours, these trailers were completely installed, configured, and ready to accept traffic.

Another dimension of the 9/11 disaster was the unprecedented traffic volume, all concentrated in and out of lower Manhattan, precisely where we had lost a major portion of our network capacity due to damage. Four hundred thirty-one million call attempts were made on our network on 9/11, which far outpaced our previous record day of 330 million call attempts. Through our Global Network Operations Center, we rerouted all traffic not directly destined for lower Manhattan, and prioritized traffic to maximize our ability to deliver outbound calls from lower Manhattan. As a result, AT&T successfully delivered 96% of Government Emergency Telecommunications Service (GETS) calls on 9/11.

Much of our effectiveness in disaster response and recovery results from our emphasis on training and practice. We run exercises of our work-center, network, and systems disaster recovery plans multiple times a year to ensure that we maintain a state of readiness. We learn from each one, and we keep our staff fresh on exactly what they need to do. This enables us to implement our plan quickly and efficiently when an unexpected event hits.

A NOTE ON CYBER-SECURITY

We treat cyber security as an integral part of our network operations model, and have invested significant resources to become the industry leader in securing our network and our customers from the full gamut of cyber threats. The diversity of our network and the services we provide has given us deep insight into the most effective means to combat cyber-crime and other threats. The raw quantity of data

[1] In order to provide continuous service in the face of a power outage, AT&T and other service providers require access to the impacted area to refuel generators and perform other tasks. Especially in connection with disaster situations, providers often need the help of the government to gain access to areas and obtain needed fuel and supplies. It would be worthwhile, therefore, to develop methods and systems, which should include necessary pre-approvals or certifications, to ensure that gaining access to critical infrastructure is a priority in any disaster scenario.

traversing our network allows us to identify and discern traffic patterns across a 24-hour day and a 7-day week. This gives us a unique ability to detect abnormalities that can suggest cyber crimes in the making. We have learned that worms and viruses rarely hit without any preceding indicators. We see the hackers testing and probing, looking for openings and vulnerabilities, and sometimes even rolling out their code on a limited basis to see how it works, days and weeks in advance of the full scale launch. Now that we understand these anomalies and how they can serve as important leading indicators, we use this information (and take advantage of the lead time it provides us) to take the action on our network and with our customers to load the filters and patches necessary to combat the hack or virus.

In this regard, AT&T is pleased to offer our new network-based security services, which help our customers migrate away from a totally perimeter-based approach. Because placing security intelligence at the edge of the network or into individual applications is costly to scale and difficult to manage, a network-based approach is often superior, as it is more nimble and efficiently distributed. One example is our offering to protect customers from Distributed Denial of Service (DDOS) attacks. A DDOS attack involves large numbers of "attackers" (mostly infected PCs whose owners do not realize anything is wrong), sending large quantities of data, all destined for the "victim" machine, ultimately overwhelming it. For customers who purchase our DDOS protection capability, we can, from inside the backbone of our network, detect emerging DDOS attacks, redirect attack traffic to scrubbers inside our network that separate the good from the bad traffic, and in turn redirect the good traffic back to a customer's IP address so that the customer can sustain operation without even feeling the effects of an ongoing attack.

I trust that the foregoing aids in your consideration of proper homeland security methods. AT&T looks forward to an ongoing discussion of these issues with the committee.

Chairman THOMPSON. I now recognize Ms. Arnold to summarize her statement for 5 minutes.

STATEMENT OF MARY ARNOLD, VICE PRESIDENT—GOVERNMENT RELATIONS, SAP AMERICA

Ms. ARNOLD. Thank you, Mr. Chairman, Ranking Member King and members of the committee.

I am pleased to address the need to broaden U.S. homeland security policy to include resilience, which in simplest terms is the ability to resume activities after an attack or after a disaster like 9/11 or after a hurricane like Katrina. At this time, I have a longer version of my testimony which I would like to submit for the record.

My name is Mary Arnold, and I am Vice President of Government Relations for SAP. SAP is the world's leading provider of business software solutions for government and for private enterprise. We have more than 14,500 supply chain management customers in all market sectors. Because business continuity and supply chain management are critical to our customers, we understand the need for information technology that provides resiliency and redundancy.

Today, much of the global supply chain's critical components are in private hands. Certainly, U.S. industry needs to take a proactive role in developing, in deploying and in exercising plans that will ensure that a disruption in the supply chain will not result in a crippling blow to their respective businesses.

Government is also a critical player. Although we cannot predict or prevent every potential disaster, we can identify our vulnerabilities in a variety of scenarios and can take steps to reduce them with the right information technology, redundancy solutions and a highly developed continuity of operations plans.

Last month, I led a panel in New York with other corporate executives on how to build a resilient nation by enhancing security and in ensuring a strong economy. There were three very important lessons learned.

First, there are no one-size-fits-all solutions. Supply chains link thousands of companies in hundreds of industries and in dozens of countries. Supply chains must work seamlessly across all of these boards. While there are core elements to all supply chains, what works for one company may not work for another. Critical components for success include flexibility, adaptivity and resilient solutions. Our public policy should encourage government and private industry to collaborate to achieve solutions that work globally.

Second, we need to take an enterprise approach to resiliency through what we might call a "resiliency chain." For example, during Hurricanes Katrina and Rita, a global chemical manufacturer required real-time information regarding goods and materials on ships scheduled to dock in Houston and in New Orleans. A primary concern was the risk to the environment should shipments become lost at sea. Because of the adaptive business network and their ability to monitor the supply chain from end to end in real time, the company was able to determine which ships were still in port, which were in transit and which had already reached Houston and New Orleans.

Within 24 hours of Katrina's hitting the gulf coast, the company received the complete listing of container shipments that had arrived prior to the hurricane. Because the software was able to show when a container leaves a port, when it reaches its destination and when it clears Customs, this chemical company was able to determine the location of their ships in harm's way and reroute them accordingly.

The third lesson: We need to consider how to incorporate our global trading partners into our resiliency chain planning. There are critical assets necessary for recovery located outside of the United States. These, too, could be vulnerable to natural or manmade disasters. Global collaboration will be necessary to ensure our ability to recover and to move forward.

The government's role in resiliency chain planning is to balance the interest of stakeholders, to set broad objectives and strategies and to provide oversight. The private sector can provide the means and the execution. By working together and leveraging the strengths of each, we can accomplish a great deal to improve our national resilience.

The private sector can be a great partner to the government in developing solutions to capitalize on existing resiliency chains. Using commercial, off-the-shelf technology products, the industry provides solutions which also reduce time, cost and complexity. Technology solutions to support resiliency chains, we believe, should have the following characteristics:

The solutions must take in vast amounts of detailed data, analyze it and return valuable information to the user. These solutions also must integrate information across many large, interconnected enterprises.

They must be based on global standards and must reflect an open architecture that can take in data from legacy systems as well as the latest technology solutions.

Finally, such solutions must be technologically agnostic. They must work with one another, open standard technologies, and not be based on one mode of communication such as a hard-wired telephone grid which may fail in a disaster.

In conclusion, securing our homeland requires the ability to respond to and recover quickly from a catastrophic event. Strengthening the resilience of the Nation must be a critical component of our homeland security policy.

In order to ensure resiliency and recovery, we must develop public-private partnerships that utilize the resources of both sectors and that play to their strengths. We must develop and deploy new technologies that will ensure that we build greater redundancy in our key infrastructure and distribution systems. Most importantly, we must put our efforts toward building public-private partnerships which provide the knowledge and tools to confront any challenge that we may face.

I commend you, Mr. Chairman, and all members of this committee for seeking ways to improve the national ability to recover quickly from a catastrophic event. We at SAP believe that resiliency must be at the center of U.S. homeland security planning, and we stand ready to participate in any and all efforts to achieve this important goal.

I would be pleased to answer any questions.

Chairman THOMPSON. Thank you very much.

[The prepared statement of Ms. Arnold follows:]

PREPARED STATEMENT OF MARY ARNOLD

MAY 6, 2008

INTRODUCTION

Thank you, Mr. Chairman, Congressman King, and members of the committee. I am pleased to be here today to speak about the need to broaden U.S. homeland security policy to include homeland resilience—the ability to resume activities after an attack or disaster like 9/11 or Hurricane Katrina.

Today, much of the global supply chain's critical components are in private hands. Certainly, U.S. industry needs to take a proactive role in developing, deploying, and exercising plans that will ensure that a disruption in the supply chain will not result in a crippling blow to their respective businesses. But, government is a critical partner in that process, and for that reason, I want to commend, and thank, the committee for recognizing the importance of this issue and dedicating the month of May to discussing homeland resilience as a core component of U.S. homeland security policy.

My name is Mary Arnold, and I am Vice President of Government Relations for SAP. SAP is the world's leading provider of business software solutions for government and private enterprise, and the third largest software manufacturer in the world. Because business continuity and supply chain management are critical to our customers, we understand the need for information technology that provides resiliency and redundancy. That is why SAP is the supply chain solution used by a diverse range of private and public sector customers, including over 75 percent of the Forbes "Global 500" companies, and public sector entities including Clark County, NV, the North Carolina Department of Transportation, the New York Port Authority and the Defense Logistics Agency, to provide them tailored resilient solutions that are flexible, adaptive and responsive. Our understanding is reflected in our over 35-year company heritage of listening to and working with our customers and experts in industries which reflect the entire spectrum of the global economy and public service entities.

Although we cannot predict or prevent every potential disaster, we can identify our vulnerabilities in a variety of scenarios and take steps to reduce them with the right information technology, redundancy solutions, and highly developed continuity-of-operations plans.

Last month, I attended and led a panel at a forum in New York along with 100 other corporate executives entitled: "Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy." In the discussions that took place there, it was clear that achieving resiliency will require a broad-based and comprehensive solution. Today, however, I am going to focus my comments on the role of information technology.

PERSPECTIVE FROM SAP

First, to state an obvious but crucial fact, there are no one-size-fits-all solutions.

Supply chains link thousands of companies in hundreds of industries and dozens of countries. Supply chain solutions must work seamlessly across all of these borders.

There are core elements, such as storage and distribution points, transportation modes, and a supplier-customer relationship endemic to all supply chains. But, there is also diversity in the U.S. and global economy such that what works for one company or industry's supply chain may not reflect the requirements of another. Thus, within every industry, we have seen the need for flexible, adaptive, and resilient solutions. We must ensure that our public policies reflect this diversity and we, as government and the private sector, must work together to ensure that solutions represent the variety of industries, cultures and companies that exist, not only in the United States, but throughout the world.

Second, we need to take an "enterprise" approach to resiliency, or what we might call a "resiliency chain" approach.

By "enterprise" I mean a holistic, all-encompassing perspective. For example, in the energy industry, our vision must go beyond rapid recovery for a single drilling rig, refinery, or pipeline. We need to look at the ENTIRE enterprise from the platform all the way to the gas pump. Similarly, in the defense industry, we speak of "factory to foxhole/flight line/frontline to factory" supply chains. That is, a perspective that reflects consideration of all the events, infrastructure, and players within that supply, or resiliency, chain.

A resiliency chain also needs to have real-time intelligence on alternatives to pieces of the existing value chain, with the existing "value chain" reflecting all the steps and players in which a product is designed, manufactured, marketed, and distributed to customers. For example, if pharmaceutical company "A" is the sole source of a key vaccine, what other pharmaceutical companies have similar manufacturing capabilities, and how could they be rapidly re-purposed in the event of an emergency?

Redundancy is one of the core elements of the resiliency chain. For example, if crucial raw materials normally move by rail, what are the backup plans if our railroads become disabled? If telephone lines go down, what are the backup means of communicating?

Third, we need to consider how to incorporate our global trading partners into our resiliency chain planning.

These partners, too, could be the primary sources of critical inputs, such as energy products; and they, too, could be crippled by natural or man-made disasters. Again, a broad enterprise perspective and global collaboration will be necessary to ensure our ability to rebound and move on.

PUBLIC PRIVATE PARTNERSHIP

What is the best role for government in resiliency chain planning?

The government's role in this context is to be the champion and facilitator of the resiliency chain, balancing the interests of stakeholders, setting broad objectives and strategies, and providing oversight. The private sector can provide the means and the execution. By working together and leveraging the strengths of each, the public and private sectors can accomplish a great deal to improve our national resilience.

Stephen Flynn at the Council on Foreign Relations wrote a fascinating article in the March/April 2008 issue of "Foreign Affairs" in which he stated that sustaining the United States' global leadership and economic competitiveness relied, ultimately, on bolstering the resilience of its society. He went on to describe a need for a sustained commitment to four key factors in order to achieve this level of resilience, which I would like to elaborate on for you today.

First, there is robustness or the ability to keep operating or to stay standing the face of danger. In a public/private partnership, we can work together and make the investment to ensure that our infrastructures, both physically, as well as operationally, are in place to deal with the challenges ahead.

Secondly, we need to focus on resourcefulness, which involves skillfully managing a disaster once it unfolds. For example, Switzerland has developed and fielded a solution which links its country's hospitals, police, fire brigades, executive staff, and the armed forces in its 26 cantons (administrative regions). Active since 2004, the solution underwent its first (and successful) live test in support of the World Economic Forum in 2005.

The third element of resilience is rapid recovery, which is the capacity to get things back to normal as quickly as possible after a disaster. Small towns and large cities across the United States are training their citizens to be auxiliary first responders. This is a perfect opportunity for the public and private sectors to commit resources and collaborate.

Finally, resilience means having the ability to absorb new lessons that can be drawn from a catastrophe. As we have seen in the wake of the September 11 attacks, we have created systems to bolster our critical transportation hubs and homeland security. The private sector is in a prime position to provide resources and play a role in implementing lessons learned.

IDENTIFYING SOLUTIONS

The private sector can be a great partner and asset to the government in developing solutions to bolster existing resiliency chains. Utilizing already developed, "commercial, off-the-shelf" technology products, that is, products with significant amounts of commercially available IT functionality already built in to them, thus reducing implementation time, cost, and complexity, we can create solutions that meet the needs and address the diversity of today's public and private sectors. When you look at IT solutions to support resiliency chains, however, keep in mind that you need solutions with the following characteristics:

- The solutions must take in, manage, analyze, and "push" back information to the user based on vast amounts of detailed data;
- These solutions also must integrate information across many large, interconnected enterprises, to become literally a global enterprise;
- These solutions must be based on global standards and reflect an open architecture which can take in data from legacy systems, as well as the latest technology solutions.
- Finally, such solutions must be "technologically agnostic." In other words, they must work with other, open source technologies, such as all types of databases, and cannot be based on one mode of communication, such as a "hard-wired" telephone grid, because that mode of communication may fail in a disaster.

CONCLUSION

Thank you, Mr. Chairman and members of the committee. Securing our homeland requires the ability to respond to, and recover quickly from, a catastrophic event, whether natural or man-made. Thus, strengthening the resilience of the Nation must be a critical component of our Homeland Security policy.

The U.S. and global economies depend on a just-in-time supply chain that is susceptible to serious disruption that can cripple economic activity. Yet today, the private sector also incorporates resiliency planning, such as keeping track of alternative supply sources and back-up transportation modes, to minimize any disruption to their supply chains.

In order to ensure resiliency and recovery, we must develop public-private partnerships that utilize the resources of both sectors and play to their strengths. We must develop and utilize new technologies that will ensure that we build greater redundancy in our key infrastructure and distribution systems to establish the foundation from which to recover after disaster strikes. Most importantly, we must put our faith in a public and private partnership which, working together, has the knowledge and tools to confront any challenge that we may face.

So again, I commend you, Mr. Chairman, and all members of this committee for seeking ways to improve our national ability to recover quickly from catastrophic events. We at SAP believe that resiliency must be at the center of U.S. homeland security planning and we stand ready to participate in any and all efforts to achieve this important goal.

That concludes my prepared remarks, and I would be pleased to answer any questions.

Chairman THOMPSON. I would like to thank all of the witnesses for their testimony.

I will remind each member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

Mr. Baker, in your opening statement, you talked a little bit about how your office promotes resiliency. Can you identify a particular department, or component in a department, which you think is an example of resilience or one that you would consider a successful model?

Mr. BAKER. I would be glad to.

I think that, in terms of allowing resilience, one effort that I would point to, which is a joint effort by the Coast Guard and CBP, is preparing for the possibility that our ports would be disrupted by an act of terrorism or by a natural disaster.

CBP and the Coast Guard have set up mechanisms by which people who are coming to a port can learn what the status of the port is and then can report back to CBP and to the Coast Guard about what alternate ports they intend to use. This allows the trade of a lot of flexibility in deciding where they are going to go based on what the market calls for; but because they are in constant communication with the Coast Guard and CBP, it allows the Coast Guard and the CBP to move their assets quickly to new ports of entry to handle the new load that would come as a result of the ship.

Chairman THOMPSON. Thank you.

I would ask some things that you think Congress, as a body, could do to promote resiliency other than what we are doing now.

Mr. BAKER. I think these hearings are a very good start.

Resilience is something that has to be part of all of the disaster planning, of all of the planning for an event; and it is something that requires that you ask in the emergency, "How can we help individuals and businesses make good decisions on their own?" There is no one solution to that, but I think drawing attention to the importance of resilience does help all of our planners address that issue.

Chairman THOMPSON. Thank you.

Dr. Sheffi, your testimony clearly states that a resilience-based approach to disruptions, including intentional, human-made attacks, is in a company's best interest.

Do you have a guesstimate of where the private sector, as a whole, is in preparing for incidents like this?

Mr. SHEFFI. The quick answer is, no. But there is such a wide range of preparedness among companies. Even today, there are companies—let me mention the good examples rather than the not so good.

There are companies like Intel, for example, that became a model of preparedness, drilling, resiliency. They even go—every month, there is a team from Intel that goes somewhere in the world, to some plant, and says, "Do you know this manufacturer of whatyamacallit part?" They are now out of business. They run the whole plant to 48 hours of exercise in trying to qualify new supplies, qualify new transportation routes. Plant managers' bonuses are based on it. Now, they do a lot of other things, but that is, you know, a very good example.

There are companies that say, "We cast our lot with the rest of them." So there is such a wide variety in what you see.

I can say that the good news here is that most large corporations are taking resilience seriously and are preparing and are drilling.

Chairman THOMPSON. Well, we heard the AT&T example——

Mr. SHEFFI. Exactly.

Chairman THOMPSON [continuing]. Of what they do.

Is there something you think Congress could do to encourage resiliency outside of government, to say, we think it is good for you to create a component for resiliency?

Mr. SHEFFI. There are two elements.

As I say, there is a redundancy element. Redundancy costs a lot of money. For example, I have been—it happens to be dangerous to be around me because I was in London and in Madrid during the attacks. The first thing that happens is, the cell phone network goes down. You cannot communicate, and the lines outside, in a public phones, the few that are there, are, you know, enormous.

Can there be some mechanism for the public sector to help the private sector invest in significant redundant capacity? Because this costs money. The part where companies know and help themselves is creating flexibility, because if one creates flexibility to be able to respond to disruption, by the same token, one creates flexibility to respond to the marketplace, to demand.

There is one thing that is clear in all markets today, which is that demand is fluctuating more and more. There is more and more uncertainty in demand. Companies that can respond better to demand, to competitive pressures, to all kinds of changes are better off in the marketplace and can increase market shares. There have been quite a few examples of companies that, during disruptions, actually increase market shares because they were better prepared.

Chairman THOMPSON. Thank you.

My time has expired. I yield to the ranking member of the full committee, the gentleman from New York, for questions.

Mr. KING. Thank you, Mr. Chairman.

Secretary Baker, if I could just ask you to look forward a bit to next December, what advice would you be giving to the incoming administration, no matter which party it is, as to what they should be doing, from the Department of Homeland Security's perspective, as far as increasing resiliency?

Mr. BAKER. I think the most important thing and the thing that is easiest to miss when you are new is the importance of planning and exercising for events so that it is not—as Dr. Sheffi said, it is not the theory of how you respond, it is a response that you have actually practiced.

As you get older, it gets harder to learn except by doing, I find, and going through exercises as a way of ensuring that the government actually has a flexible response is probably the most important thing that a new administration can do.

Mr. KING. I know the Department has made a concerted effort to increase cooperation between Federal, State and local governments as far as sharing intelligence, as far as working together to head off attacks.

When it comes to the issue of resilience, how much cooperation is there between DHS, the State and local governments and the private sector?

Mr. BAKER. I think our cooperation is good through fusion centers. We have come to know a lot of the participants in this process.

As you know, the Congress created an Assistant Secretary for State and Local Law Enforcement. They have put that office in my office. We have appointed Ted Sexton, a former sheriff from Alabama, to that job. His first task is to look at the question of how do we build resiliency for law enforcement so that neighboring jurisdictions can supply law enforcement packages to communities in need on a fast basis but on an organized basis, so that it is not just individual police officers showing up without support.

That is something that we are working on and expect to have a proposal for in the next few months. So that is something that, I think, will add greatly to State and local cooperation with the Federal Government in providing the fundamental order that allows people to go at the business of recovering on their own, bouncing back from a disaster.

Mr. KING. I do not want to turn this around on Secretary Baker, but do any of the other panelists—can they suggest what the Department should be doing that it is not doing or, say, what the Department next year should be doing to continue this effort?

Mr. Southers.

Mr. SOUTHERS. Yes, sir.

On two fronts, first on the Centers of Excellence, I have the very unique opportunity—in addition to being Chief of Intelligence in Homeland Security, I am also an Associate Director of the Center of Excellence at USC.

One of the things that we have done is, we have leveraged their research capabilities, what we are calling "translational research," research that is going directly from the laboratory to the field and to the people who are operational.

You have got 13 Centers of Excellence that, with all due respect, probably house the best and brightest people in this country who are researching homeland security solutions. I think we should, perhaps, leverage those Centers with our critical infrastructure sites that need that capability and that knowledge to test out possible solutions for resilience, should we have a man-enabled or a natural disaster.

The second item is in the area of intelligence. It might be a wise suggestion or move to embed our regional security advisors, meaning the protective security advisors, TSA and surface transportation advisors, within the local fusion centers.

We have the unique fortune at LAX of having every section or every agency of government at our airport, and so our relationship and our communication in terms of intelligence is pretty seamless. But I think if we were able to embed these folks into the fusion center we would then be able to enhance our risk-based decision-making with intelligence-led decision-making, as they are doing in London and in Israel.

Mr. KING. Dr. Sheffi.

Mr. SHEFFI. It is something more specific, maybe because I was born in a different country and I spent a lot of time in Europe.

I was struck in the United States by the amount of volunteerism after a disaster and by how uncoordinated it is. There is a huge outpouring of goodwill and support that is not being captured. It happens in every big disaster in the United States. You see it, but there is no mechanism to capture it, to coordinate it and to use it.

In addition to this, as far as the private sector is concerned, provide some type of regulation, some type of incentive for drilling and some type of auditing that verifies that companies are drilling and testing and that they are, you know, coming up to the standards of AT&T and of other good corporate citizens.

Mr. KING. Thank you, Doctor.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

We now recognize the gentlelady from Texas for 5 minutes, Ms. Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, let me thank you very much, and I thank the witnesses as we probe this topic.

I do not think there is, certainly, a more important aftermath than the ability to get back up on your feet. It seems to be an American challenge. Certainly, we would like to think it is an American value as well.

Let me just start quickly—and I have a series of rapid-fire questions, Ms. Arnold, just to ask you directly.

Do you think the Department of Homeland Security has adequately focused on promoting resilience? Do you think the word is out that getting back on your feet is just as important as being able to counter the attack that may come, but that resilience in starting back up is crucial? Do you get a sense that there is that kind of focus at the Department of Homeland Security?

Ms. ARNOLD. I do believe that both Congress and the Department are keenly aware that this needs to be addressed, and there is an understanding that there needs to be a collaboration and a streamline of communications.

Ms. JACKSON LEE. What do you see specifically that gives you the sense that that is happening, in that you are giving me that response? What is there concretely that suggests that that is the case?

Ms. ARNOLD. Nothing other than just conversations with staff at this point.

Ms. JACKSON LEE. Let me move to Mr. Baker and ask the question about resilience and for you to give us some of the examples. I guess you stated some of them in your statement, but some—again, concrete examples and then results of the agency's emphasis on resilience.

Mr. BAKER. Yes. Thank you.

As I said, we think that in many cases the key to resilience is to give people good information and to make sure that they have the freedom to act on that information.

In the business context, where we are thinking about resuming operations at a port, we have an established mechanism for doing that. The same is true for ports of entry.

We are all quite aware of the importance of the U.S.-Canada border economically and of the smooth flow of traffic across that border, even after an event, on the question of how will we resume traffic if there has been any interruption. Again, we have protocols designed to make sure that information gets to people who are coming across the border so they can plan, so they can adjust on their own to changes as a result of a natural disaster or an act of terrorism.

Ms. JACKSON LEE. Let me just ask if you could submit in writing maybe some concrete broader responses to resilience that relates to a broader sector. I will just leave that on the record——

Mr. BAKER. I will be glad to do that.

Ms. JACKSON LEE [continuing]. And ask that you have that in writing.

Let me ask Dr. Sheffi, and I know his name has been pronounced in many different ways, but let me welcome you——

Mr. SHEFFI. Sheffi is fine.

Ms. JACKSON LEE [continuing]. And ask quickly if you look to New Orleans and you look particularly to the healthcare sector, there is no effectively running hospital. The public hospital is not open. What is your response to DHS's focus on resilience, and do you think that is a good showing of resilience when a city now 3 years late does not have a functioning public health sector?

Mr. SHEFFI. Tough question. I can only say that I was in Europe during New Orleans, and I thought it was al Qaeda propaganda, the thing they were showing on TV. So the magnitude of the failure was breathtaking, still going on. I actually don't think that the department of government in large part has been focusing on resilience. In large, it is totally understandable. Most defense forces, most governments think in terms of prevention, preventing an attack. That is what the public wants, the government to prevent it. It is actually, as the chairman said before, it is talking truth to the population, saying, look, we will not be able to prevent it 100 percent. That is not a stance that many executives like to take, because in some sense even talking about resiliency is admitting that failure is an option. It is much, much better——

Ms. JACKSON LEE. So you think we have cracks in the armor? When we don't have a functioning hospital system that means we have a weak response in resilience?

Mr. SHEFFI. Of course.

Ms. JACKSON LEE. My time is short. So Mr. Southers, let me quickly ask you your experience regarding resilience in other countries where there have been terrorist acts. Do you have any sense of that that could be helpful to us?

Mr. SOUTHERS. Yes, particularly in Israel they have a natural resilience. Everyone there is a first responder. Should there be an incident, everyone understands what to do. Their most important function in that country is a psychological impact that is going to be minimized by getting operations back in order. Same with London and the bombings that they had there. Getting things back in order is very important. So one of the things that we are trying to do here, as we respond to threats, we understand that threats can actually cripple the aviation domain. We are trying to be more intelligence-driven so that we can minimize the disruption and mini-

mize the economic consequences of an attack or the threat of an attack to our aviation system. So those two countries in particular are certainly models of resilience as it relates to man-enabled disasters.

Ms. JACKSON LEE. I think we can look to those for guidance. I think there needs to be a resilience policy defined at the Department of Homeland Security. I yield back to the chairman. Thank you.

Chairman THOMPSON. Thank you, Ms. Jackson Lee. I now yield 5 minutes to the ranking member, Mrs. Miller.

Mrs. MILLER. Thank you, Mr. Chairman. I like the sound of that very well. Thank you. I might pick up, Mr. Baker, with a comment you just made when you were responding to my colleague about the smooth flow of commerce between the United States and Canadian border, because I come from Michigan, of course, a border State. In my immediate vicinity, we have the Ambassador Bridge, which is the busiest commercial artery in the northern tier of the Nation, with a tunnel to Windsor underneath the Detroit River.

In my immediate district we have the Blue Water Bridge, which is the second busiest commercial artery on the northern tier, and is the only one where you can transit hazardous material, as well as the CN rail tunnel that runs under St. Clair River, which is the busiest rail entry into our Nation. Immediately across the St. Clair River, if you are a good golfer you could hit with a golf ball—I couldn't, but somebody who is a good golfer could hit the largest concentration of petrochemical plants I think outside of New Jersey in our Nation as well.

So we have a number of unique dynamics there. My question is going to go to how the Department actually works with the local communities, with the local counties, the States in particular on their response mechanisms and their planning process. It is my understanding that each of their respective States are responsible for constructing their own plan in regards to identifying soft targets, available resources that they may have, et cetera. I am just wondering how does the Department work with the various States in critiquing those plans? Do you do periodic updates? What can Congress do to assist the Department and the States?

Mr. BAKER. We do work closely with the States on their plans. We review them, we talk to them about them. We have to recognize that in an emergency, the State is the first responder. The local government is the first responder. Governors are quite jealous of their own authority to respond, and have a great confidence in their ability to respond. So we have to defer to their initial decisions about how to handle particular emergencies. But we have also learned the importance of having a very good plan that has been properly reviewed and exercised. We work closely with the States to encourage them to do that. We provide funding that assists them in preparing those plans. Then through fusion centers and the Homeland Security advisers, we provide a great deal of intelligence about the nature of the threat that they ought to be responding to and preparing for.

Mrs. MILLER. I just raise that question because I mentioned to you about the Blue Water Bridge. Several years ago, I personally went and looked at the viaducts, the underbody of the bridge on

the Canadian side, where they had concrete embankments around all the viaducts. It appeared to me from a layman's term that they were fully prepared. Yet on the American side, on the Michigan side there was nothing. I personally called the Department of Transportation and said for goodness sake, get some concrete embankments around here. You could imagine if someone blows up one of these viaducts what it would do to the economics of the Nation, because both the genesis of I–69 and I–94 are at the foot of that bridge as well, obviously huge trade routes.

So I just wonder how the committee worked with that. If I could, because I am running out of time here, I was very interested in your reference about the reverse 911. Could you sort of flesh that out for me a bit? Is this something that is just working in California? I wasn't familiar with that. Is it happening around the Nation?

Mr. BAKER. It is technology that was developed privately by a company that is now being rolled out in a variety of places. I think the company is from Indiana. It is a very valuable opportunity to communicate with citizens. But it is really just the beginning. All of us now carry cell phones that are capable of receiving messages that are targeted to at least broadly the location, because the cell tower we are all in communication with is a local spot that can be identified. It is true that cell phones stop working in emergencies, but text messages are much more likely to get through. Developing mechanisms and standards for communicating to people in an emergency what we know using text messages and perhaps getting text messages back is something that we are exploring quite actively right now.

Mrs. MILLER. Thank you very much. I guess I have 20 seconds left, so I will make one comment to Dr. Sheffi as well. I appreciate your comment about all the volunteerism that America has and throughout generations it has always been part of our strength. But I would say that I think the American Red Cross is a mechanism that we have put in place. Obviously, in the largest room there is always room for improvement. But the American Red Cross does a remarkable job in times of need to try to harness some of the volunteerism and shift those resources where they are necessary as well. I just want to make that comment as well. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you. I will now recognize the gentleman from Pennsylvania for 5 minutes, Mr. Carney.

Mr. CARNEY. Thank you, Mr. Chairman. Professor Sheffi, testimony from AT&T asserts that the metric for being resilient is resumption of activities within 72 hours. Does that metric make sense to you?

Mr. SHEFFI. Can we go to the next—no. Seventy-two hours may be obviously too long. One has to leave within 1 minute. AT&T understands their own technology better than anybody. The question is really what would it take? You want to get back within, you know, 72 seconds. The question is, is it technologically feasible? It is actually easy. Some of it is technologically feasible. The question is the price and who will pay for it. So when one said is 72 hours enough? No, it is never enough. One can always do better. But every company has to balance, you know, risks, shareholders, cus-

tomers. AT&T, like any other company, I am sure does this type of balance. The role of the government, coming back to one of the questions before, is the government can actually tilt the balance. The government, through various actions, regulations, taxations can move AT&T and corporate companies like it to change their calculations about where the balance should be.

Mr. CARNEY. Ms. Arnold?

Ms. ARNOLD. Yes.

Mr. CARNEY. I am over here. How do you quantify whether SAP is resilient? What metrics do you have?

Ms. ARNOLD. What I can tell you how we look at our software solutions are very holistic, enterprise-wide from the tree top level down to the most granular down to a bin in your warehouse. Most of the software is provided with automatic alerts. So rather than waiting for a full-blown issue to arise, what we find with our software is that in many cases you are alerted to a small glitch before it becomes a major problem. Then as it escalates, if it shouldn't be solved at that level, then everybody from the plant manager all the way up to the CEO can be notified.

One of the things that SAP does in our software is go through various scenarios. What if this? What if that? What are other suppliers if this supplier goes down? You can actually have visually go onto your plant floor and if you have an engine that is overheated in a critical part of your manufacturing plant, you can then switch that engine off and then go to another. So I guess what we would argue that we provide is real-time data to our customers as possible so that they can react quickly and collaboratively and with all of their partners.

Mr. CARNEY. Is that resilience or is that just standard operating procedure? I mean, resilience seems to me being able to bounce back after something happens.

Ms. ARNOLD. Sure.

Mr. CARNEY. What is the metric for that that SAP has?

Ms. ARNOLD. We would say from a resilient standpoint again is having redundancy. Again, when you have—we break out the whole solution so that when a company is making their planning processes, if supply A goes away, then generally they will have the ability to have identified supplies B, C, and D, and not miss a beat if supply A goes down.

Mr. CARNEY. Okay. Thank you. One more question. From your point of view, do you think that DHS is adequately focused on promoting resilience?

Ms. ARNOLD. I think that the Department of Homeland Security is extremely sensitive to what is going on, and is certainly addressing, making every attempt to address those needs at this point. I think that the dialog is just beginning and will continue to do so.

Mr. CARNEY. So that is a yes or a maybe or——

Ms. ARNOLD. I think everybody involved is trying to do the best they can would be my answer.

Mr. CARNEY. Okay. Mr. Southers, just a quick one, can you provide us your assessment of the quality and timeliness of the intelligence, the information you receive from TSA and DHS, intelligence community, et cetera?

Mr. SOUTHERS. The timeliness that we have at LAX is quite extraordinary. We have officers that are in the fusion centers on both the Joint Terrorism Task Force and the Joint Regional Intelligence Center. They certainly could be enhanced, as I mentioned earlier, if some of the DHS assets were embedded in those centers as well, and also if some of our officers were given additional opportunities to staff those centers. But it has been seamless as a great result due to the Joint Terrorism Task Force and the fact that we are actually sitting in the same room sharing the information.

Mr. CARNEY. Thank you. No further questions, Mr. Chairman.

Chairman THOMPSON. Thank you. We now recognize the gentleman from New Jersey, Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman. Dr. Bailey, AT&T, do you have the State and local and Federal Governments participating in your exercises?

Ms. BAILEY. Sometimes we do. You are referring, I believe, to our network disaster recovery exercises.

Mr. PASCRELL. That is exactly what I am referring to.

Ms. BAILEY. Frequently we do. In fact, we had in an exercise that we held in the Washington, DC metropolitan area about a year or two ago, we had participation from the Department of Homeland Security specifically to trial some credentialing technologies and capabilities.

Mr. PASCRELL. Do you share information with the Department of Homeland Security?

Ms. BAILEY. Yes. Absolutely. We share—in fact, we hosted a commission from DHS just last week up to our global network operations center. I personally participated in that meeting with Secretary Jameson to share our approach, our challenges, and leverage DHS. I also do want to comment on the very good support we get from DHS as it relates to the sector coordinating council for telecommunications.

DHS operates something we call the NCC NCS, national coordinating center for telecommunications. It is identified as the telecommunications coordinating council participating—you know, participants include all the major carriers as well as DHS officials. It has been in existence for many, many decades. It has served to be extremely helpful in preparing us and enabling us to coordinate to be prepared, as well as to coordinate after an event, to share information, to get information about, for example, in Katrina where exactly is the water so that we cold see what pieces of our infrastructure might be vulnerable. DHS has recommended expanding the notion of those sector coordinating councils across all the major critical infrastructures. I highly support that kind of an approach. It has been very helpful.

Mr. PASCRELL. Secretary Baker, I believe since the attacks of September 11, 2001, we have all said that it will take a truly multi-faceted approach to keep our Nation safe in the face of numerous threats. That, I assume, is, hopefully, and the committee believes this, a bottom-up approach that involves the community, regional planning, excuse my back, I am over here, and trained volunteers, talking about the doctor mentioned volunteers. There are two issues I would like to talk to you about. There is a story in the paper today, USA Today, let me read you the headline, "Hospitals

Can't Handle Attack". Very interesting review. This is one aspect of it, but I think it is very, very, very reflective. They can't even withstand an attack from a modest—a modest terrorist attack. In fact, of the numerous cities that were involved, the seven major U.S. cities, Washington, Minneapolis, Los Angeles, Chicago, Denver, Houston, New York, they have a total of about 100 beds were vacant on the day they chose to do this test, March 25 at 4:30 in the afternoon. This is a disaster. It is not acceptable. We knew about it 6 years ago. There is no resiliency here whatsoever.

These are hospitals that were very interested in serving. But what is more interesting is that this administration wants to cut Medicaid dollars, which in the words of Irwin Redlener, who is director of the National Center For Disaster Preparedness at Columbia University in New York, would even make matters even worse. We have a, he says, a really serious catastrophic acute event, a nuclear detonation or widespread chemical attack, we have thousands of victims simultaneously, there is no urban area that is prepared for large scale disasters. Why under those circumstances, Mr. Baker, would the administration be recommending cuts in Medicaid, which will only make this situation worse and exacerbate it?

Mr. BAKER. Well, as DHS's policy director, I have got a lot of responsibilities. Medicare isn't one of them. But I do want to answer your question.

Mr. PASCRELL. We are all working together here, aren't we?

Mr. BAKER. We are.

Mr. PASCRELL. Is this the Homeland Security Department that is looking at its own responsibilities over here and the administration is talking about an umbrella or comprehensive—and certainly it impacts you.

Mr. BAKER. It absolutely does. We are committed to planning for a disaster, including a nuclear detonation.

Mr. PASCRELL. How are we doing in hospitals?

Mr. BAKER. We certainly, as you heard Dr. Sheffi say, building redundant hospitals that will sit there waiting for a nuclear explosion is not an answer to our needs. We will have to respond by using every available facility, including prisons and schools as hospitals——

Mr. PASCRELL. Are there such plans to do that——

Mr. BAKER. There are plans to do that.

Mr. PASCRELL [continuing]. Secretary Baker? There are no such plans, Mr. Baker. Mr. Baker, let me tell you something very important. Forget about attacks from the outside, you know, from some foreign nut case, let's talk about what is happening in the United States if we had huge disease spread out over the United States of America or in any particular section. Our hospitals are not ready to take care of that. Where is the resiliency there?

Mr. BAKER. I asked our director of health affairs about that. I said does the fact that the emergency room is full mean that you don't have an ability to respond to a disaster? He said not necessarily. I had a plane crash when I was running a county emergency system, and I called up the hospitals, and I said we have a plane crash, we need—immediately, we need beds. What they did is they stopped all the elective surgery for the next 3 days and they immediately freed up beds. Now they can't do that every day.

Mr. PASCRELL. Do you know how many beds were available at that particular time in March in Washington, DC, where we are sitting? Do you know how many beds were available?

Mr. BAKER. I don't know the number.

Mr. PASCRELL. Zero, nada, nothing.

Mr. BAKER. I will also bet you that there were people in beds——

Mr. PASCRELL. That we could put out of beds, throw them out of bed.

Mr. BAKER [continuing]. Did not have to have surgery.

Mr. PASCRELL. How many people you think we could do that to? You have any idea how many people we could do that to?

Mr. BAKER. My understanding is there were a large number of beds were freed up by that.

Mr. PASCRELL. The resiliency, Mr. Chairman, is a beautiful word, multiple syllables, sounds good, very important. Very significant. I like the word. I like the etymology of the word, too. I won't go into that now. You talked about redundancy and flexibility. Hospital systems do not have that. The hospital systems don't have the luxury. If they don't get help—not only are they not going to get help, we are going to cut Medicaid. We are going to make it worse. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you. The gentleman from New Jersey makes his point, as he always does. The gentleman from North Carolina, Mr. Etheridge, for 5 minutes.

Mr. ETHERIDGE. Thank you, Mr. Chairman. Let me sort of change the conversation to a little different area, but it deals with the same problem. Because I am always interested in how homeland security can address the safety and security of schools and school children, because they are part of this country. A critical part we tend to forget in New York, the schools were disrupted and children were for a long period of time. We didn't hear a lot about that, but it was. Specifically, whether it be a natural or manmade, it is still a problem. Because it is important to get communities back flowing and working. If you have children, parents understand that very quickly. For communities it is a critical piece because it is part of the resiliency.

If you look at what has happened in New Orleans, schools still aren't operating, children aren't in school in some places. If you go to Houston, they are overcrowded. They still have the problems. So my question is this, Mr. Baker. How is DHS looking at resiliency as it pertains to school and the need for communities to provide essential services after a disaster? But also to prepare for it before it happens?

Mr. BAKER. We strongly recommend and support, including with funding through UASI and other programs, planning for a disaster that will affect a particular city. So that the cities who are having the responsibility typically for education will——

Mr. ETHERIDGE. No, sir, it is not the cities.

Mr. BAKER. The local governments that have the responsibility for the schooling of our children——

Mr. ETHERIDGE. But the Federal Government has the responsibility for the overall broad planning.

Mr. BAKER. We do have responsibility for making sure that there are plans. It is important, as I said when I was making my earlier

statement, that we recognize that if resiliency depends on some central government making all the decisions, we will always have a brittle system and not a resilient system. We have to allow local decision-making, the creativity to respond to local conditions. That includes the creativity to come up with particular solutions that reflect the educational institutions that are in the area.

So we encourage local planning for local disasters, and then we will back the schools up and we will back the communities up with Stafford Act funding and responses in the event of an emergency. We can help them with the planning. We can't do and shouldn't do the planning for them.

Mr. ETHERIDGE. Thank you. You are aware there is Federal legislation that requires Homeland Security to provide a template for schools to look at. I assume you are aware of that.

Mr. BAKER. Yes.

Mr. ETHERIDGE. They would also include in the legislation to make it available for the planning that has been introduced this year, I hope you take a look at it, to provide for some resources. It is one thing to do the planning, but if you don't have the resources the plan doesn't work too well. So I hope you look at that. Mr. Sheffi and Ms. Arnold, how can we help schools reduce vulnerabilities and improve the resiliency that we are talking about? What analysis is necessary to determine, I guess to determine where vulnerabilities can be reduced or mitigated? How can we work to develop plans for schools to bounce back after we have these disasters? You talk about how important it is. So what are some of the things we can do or should be doing?

Ms. ARNOLD. Congressman, I think one of the things that I would suggest is that you look to the country of Switzerland. Switzerland about 3 years ago built a centralized system to coordinate medical response to large scale crises. During that program, what that they pulled together was their fire brigades, their medical teams, their first responders, their emergency control centers, and they centralized it into one Web-based scheme. They found, they did a medical analogy, that most people suffer the gravest injuries within the first 60 minutes of being injured. So their main mission was to get people treated before 60 minutes was up.

When they first started out, they literally had to make, as somebody said earlier, phone calls to say do you have a bed in your district because I have got a burn victim or I have a car fatality, blah, blah, blah. Once this became automated with the supply chain management system you had an end-to-end visual of where your hospital centers were, where your fire brigades were, and you could deploy them in the most fast and effective means. You could determine, based on the casualty, which hospital was best suited to take the injured individual. Also the first responders were able to look at what we call the standardized best practice. So, you know, if this then do that. So we kind of brought everybody into the mode. Then on top of it they were able to manage their beds. I thought about that example as I read that article this morning about our beds being in such short supply.

So I really think what needs to happen is a centralization, a standardization of data going into that central repository that needs to be easy to use so that all levels can tap into it, and it can

be Web-based, and that there need to be, you know, some standard practices. And that you have a full and real-time scenario of where your assets are and how you can best deploy them. Whether it is a school system or, God forbid, a flight go down, you can see how this is very scalable. In fact, it went live in 2005, and they did a demonstration at the World Economic Forum in 2005. So there are examples. I will grant Switzerland is a very small country, they only have 26 as they call it cantons or administrative regions, but I do believe there are some lessons to be learned, and ones that we can import back to this country.

Mr. ETHERIDGE. Thank you.

Chairman THOMPSON. Thank you very much, Ms. Arnold, and a staff member will talk to you a little bit after the hearing about some information on that subject.

Ms. ARNOLD. Sure.

Chairman THOMPSON. We will now recognize the gentlelady from the Virgin Islands, Mrs. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman, and thank you for this hearing, because resiliency is, I think, where we need to be focusing. We know that you can't protect us 100 percent, prevent 100 in bioterrorism. We know we have no clue what the bug might be or how it might be altered. Both from real-life experiences and from some of the exercises that we have held, we know that our weakness has been in recovery. And that is resilience. We have seen the Department move away from things like something that I know from my district Project Impact, where we set up public-private partnerships ahead of time to mitigate and to, you know, strengthen the ability to be resilient in communities.

So that is—I am glad we are having this hearing. I want to go back, as you can imagine, to the hospital issue. In most of those situations, not only are there no beds, but there are people in the emergency room waiting for beds. So, you know, it is not really that easy to move people around. But every time we look at the Department's budget, the budget for health and the part of the budget set aside for health and hospitals does not reflect the importance of helping our hospitals to become resilient. Are you seeing any change in that as we get ready for next year?

Mr. BAKER. I will be glad to address that. I think that we have reflected in the last few years the importance of the health issue and the resources that are brought to bear in the event of a bioevent of some sort, including a natural infection. We created an Office of Health Affairs. The budget for that has increased significantly, and it has been given new authorities in the last few years.

Mrs. CHRISTENSEN. We appreciate that. But it doesn't help us out in the different cities.

Mr. BAKER. Yes.

Mrs. CHRISTENSEN. I remember going to Oakland Highland Hospital, a level one trauma center, and yes, I asked them—this is a couple of years ago. They got maybe a couple hundred thousand dollars. It doesn't go very far.

Mr. BAKER. As far as that goes, we don't have the ability to say we should have twice as many hospitals, we will fund them and have them on the shelf waiting for an event. We have to encourage local governments and States to plan with the resources they have

and to come up with a mechanism for dealing with emergencies. I would just say while I don't pretend to be an expert, I think HHS knows much more about this than I do, about the ins and outs of particular hospital availability in the event of a crisis, the fact is that every hospital, even if they have a crowded emergency room, has elective surgery candidates who are showing up every day. I know I have had shoulder surgery probably 5 years ago, and if somebody called me up and said we have had a plane go down and we have given your bed to somebody who was burned in that accident, I would have understood and waited another 6 months for shoulder surgery. So we do have some capability to respond to an emergency.

Mrs. CHRISTENSEN. Well, I hope that, Mr. Chairman, that we could have a hearing just devoted to this issue. Are you familiar with the system or that room that Secretary Tommy Thompson had set up where we are supposed to be able to know hospital bed capacity in every hospital in every State, city, and be able to utilize that in a disaster emergency?

Mr. BAKER. I have seen the——

Mrs. CHRISTENSEN. Is it operational?

Mr. BAKER. I have seen the Health and Human Services intelligence center, which is operational. If that is what you are talking about, I have been to it. It is in operation. I don't know whether it has all of the information that you talked about.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. We now recognize the gentleman from Washington State, Mr. Dicks, for 5 minutes.

Mr. DICKS. Well, after listening to this discussion about the hospitals, Secretary Baker, you get into the question about anthrax, and a possible—that kind of an aerosolized anthrax attack. Your point is well made that what we really need is to have the individuals have this medicine to be able to take. How many people have this? Nobody has this, right? I mean this is a theory, or this is what we would like to have. But people—do people actually have these drugs or can they get them? I mean can Members of Congress, you know, go to wherever we go and get a handful of these things?

Mr. BAKER. I wouldn't recommend getting a handful.

Mr. DICKS. Well, whatever the appropriate dose is.

Mr. BAKER. I don't want to go into too far into territory that is really the responsibility of Health and Human——

Mr. DICKS. It is in your stable.

Mr. BAKER. Yes, and our job is to be prepared for an attack and to think about——

Mr. DICKS. We are not prepared for it.

Mr. BAKER. We have a rather detailed plan for delivering countermeasures, including cipro and doxycycline to the area where an attack has occurred.

Mr. DICKS. But as you say, if you don't get them within a matter of hours, it doesn't make any difference.

Mr. BAKER. This is——

Mr. DICKS. So in those cases, I would go back and argue that maybe prevention and deterrence, whatever way to stop this from happening in the first place, is just as important as resilience if re-

silience is not possible. I mean, maybe in the telecommunications area you can restore something in 72 hours. In this area, unless you give the people the pills within a matter of hours, they are going to die.

Mr. BAKER. I could not agree more. I share that concern.

Mr. DICKS. So prevention is a lot better option to me than something—I mean, you can call it resilience, whatever you want to call it, but it is not going to work and people are going to die.

Mr. BAKER. The faster we can get these countermeasures in people's hands after an attack the better. While we do have a plan for delivering them, having them actually on hand in the home, in the office is a very prudent step for people to take. I want to be cautious about that, because having antibiotics on hand and taking them for something other than a serious event could build resistance to antibiotics, which of course is a major concern of the public health community. They have been very cautious about recommending that people keep these stores in their home. We are working with them now to see if there isn't an appropriate solution to that problem because of the importance of responding very quickly to an aerosolized anthrax attack.

Mr. DICKS. How many years do you think it will take to get an answer?

Mr. BAKER. I am hoping for an answer in months rather than years.

Mr. DICKS. Does anybody else out there want to comment on this what I consider to be a dilemma? I mean, if you can't—I mean, to me it seems as if prevention in this area is critical. Maybe some areas, you know, telecommunications, yes, you can restore that and it is not the end of the world. But in some areas, you know, if you don't prevent the accident, a lot of people are going to die. Just as the gentleman from New Jersey points out, we don't have—I happen to be one of those people, by the way, I was having an operation when I was 24 years old. I was actually on the operating table and there was an earthquake in Seattle. The dust fell, and the paint fell, and they took me out and they opened up the facility in case there were emergency victims. So that does—that can work. But that would be such a small number of beds. If you had a catastrophic attack on Washington, DC, I am not sure that policy is going to get you very far.

Mr. BAKER. Absolutely. We would have to turn to a whole host of other alternative institutions.

Mr. DICKS. Well, Mr. Chairman, resilience may be the word for the day, but I am for prevention. I think prevention still should be up there at the top of the list. Thank you.

Chairman THOMPSON. Thank you very much. I now recognize the gentleman from California for 5 minutes, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I appreciate this hearing. Though I have not been here, I have gone through the testimony of the witnesses. So let me ask somewhat of a general question. That is this. With certain elements of our private infrastructure, the immediacy of getting their function back up is part and parcel of what they do. Financial institutions, if they were disrupted for more than 24, 48, 72 hours, it really affects them. So it seems to me that building in resiliency to make sure that doesn't

happen can be justified as part of the bottom line. Similar with telecommunications companies. But there are a whole other set of infrastructure in the United States where the immediacy perhaps is not such that it would be readily apparent and accepted in the bottom line. So what do we do as a government to work with the private sector, or what incentives do we need or what regulatory mechanisms do we need such that resiliency as understood in today's discussions would make sense from a corporate decision-making standpoint to go to the bottom line? I hope I am clear on that question. But it is one that has intrigued me for some time. On the one hand, we understand that 85 percent or whatever the number is, 85, 87, 90 percent of critical infrastructure is actually owned by the private sector. But sometimes the kinds of things that we need to do to protect against terrorist attack or to respond to a terrorist attack or other kind of abnormality which would cause disruption is difficult to calculate in the bottom line, and I presume for corporate leaders to be able to justify to their stockholders. Therefore, it seems to me there must be a role the government should play, but I am not sure exactly what that should be. I wonder if the panelists might have a comment on that.

Mr. SHEFFI. I will try to answer. First of all, I am not sure that there are such assets. In today's, we have gone through 20, 25 years of making corporations very lean and very, you know, using low inventories, using just in time, which means that assets are utilized extensively, which means that whatever the company is doing, whatever the enterprise is doing is geared toward, you know, adding value and adding to the bottom line. So it is not clear that there are examples where assets are just standing there, yet they are important for national resilience and companies wouldn't care about it.

It is not clear that this is a big concern. Because whether it is, you know, AT&T Communications or, you know, a manufacturing plant or a warehouse or distribution center or store, if Wal-Mart loses a store, they would lose revenue. So it is not clear that there are many assets in the private sectors that are not tied directly to the value stream of that company.

Mr. LUNGREN. So in other words, you don't think there is anything the government needs to do to raise the visibility of that issue to corporate America in the area of infrastructure?

Mr. SHEFFI. No. We talked before about an example that AT&T raised, that they have 72 hours to come back to the same level of service. My comment was why 72 hours? Why not 71? Why not 75? Is 72 hours a good number? But the issue is with the current incentives that the government provides through taxation and regulation they chose 72 hours as a combination of what they can do with the current technology, what customers expect, what they think are their corporate social responsibilities. However, if the government would make a statement that, you know, 41 hours, you know, is the right number, and have some both regulations and incentive to do it, they would change the calculations of AT&T or other companies. If the government thinks that getting supply of, I don't know, Campbell's Soup is important, so Procter & Gamble would change its calculation in how it thinks about resilience. So the government certainly has a role. The government has to decide

what is important and how important is it. Do we want it back in so many hours, in so many days? What kind of disruption? Let me stop there.

Mr. BAKER. I think you have put your finger on a very good point. It is very hard, though, for the government to have an overarching standard for exactly how resilient a particular industry ought to be, because that will change as people's perception of the risk changes. The financial institutions that today have warm backup centers that are ready to take over all their transactions in an instant did not have that on September 11. It was only the realization of how at risk they were that led them to adopt much more extensive redundant systems.

On the other hand, the market punishes failure to prepare for this and rewards a company that prepares. Wal-Mart did an excellent job of responding to Katrina using their very extensive IT system so that they had people and stores and delivery trucks ready to reopen almost immediately after the hurricane passed through, and as a result, made a lot more money than their competitors who were slower off the mark.

Mr. LUNGREN. So at least one of the things the government ought to do is be as transparent as possible given the fact we that don't want to give away intelligence secrets, but to inform those who have critical infrastructure as well as the general public that the nature of threats, the extent of the nature of that threat, and so forth.

Mr. BAKER. I think that is exactly right. We can point out threats that the private sector may not be aware of, problems that we see. We have recently addressed the question of what would happen in the event of avian flu, a pandemic in which everybody should stay at home and work from home. That is fine. That is a great new technology that we can use to avoid people coming into contact with each other unnecessarily. But right now the telecommunications infrastructure does not fully support that. We need to address that.

Mr. LUNGREN. Thank you.

Chairman THOMPSON. Thank you. The gentleman's time has expired. We now recognize the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. I thank the witnesses for the testimony that we have heard. Ms. Arnold, if I may, do you have a person within your operation who is charged with resilience implementation?

Ms. ARNOLD. We actually have a number of—not one specific person who is charged with resiliency, but we divide up the industries into 26 sectors and then we work——

Mr. GREEN. If I may do a quick follow-up. I asked about a specific individual because if some branch of government wanted to contact your company, would that person then call 26 different people or is there a person that would be called?

Ms. ARNOLD. If it was public sector, yes, there would be a public sector person that you would call.

Mr. GREEN. So you do have a person that is available for the Federal Government to contact?

Ms. ARNOLD. Correct. If they want to talk about public sector solutions.

Mr. GREEN. Does that person have someone at the Federal level that he or she can immediately contact, a name and means of contact, communication with someone at the Federal level that is already known to you?

Ms. ARNOLD. I am not sure I understand the question.

Mr. GREEN. Well, what I am getting at is if you needed help——

Ms. ARNOLD. Yes, sir.

Mr. GREEN [continuing]. And you wanted to get over to someone at the Department of Homeland Security, do you now know the name of the person or the organization that you would immediately call? Is that already in place?

Ms. ARNOLD. We work extensively with Customs and Border Patrol, yes, sir.

Mr. GREEN. I will take it from this answer that you are not giving me a yes or a no. I am not trying to press you too hard. But is there a person that you—some person that you are to call, some agency that your person already is aware of that he or she contacts?

Ms. ARNOLD. Generally, our folks with the chief technology and chief operating officers for the departments and agencies.

Mr. GREEN. Is there a codified plan in place such that in the event of some unforeseen ugly circumstance your person knows that he or she is to call this person with the government?

Ms. ARNOLD. In the case, for instance, of Customs and Border Patrol, yes. There are several folks that know to—they work in concert. We work on a daily basis.

Mr. GREEN. I am asking this line of questions because it seems to me that the web of resilience should be woven such that there is some sort of interconnectivity between public and private and the government. There ought to be some web that causes each business to have a means by which it can communicate up the line to some other person. Is that web in place?

Ms. ARNOLD. That web is in place. Actually, we have services folks that are dedicated to a department and work hand in glove with them if they have an SAP solution and running that. If there is, in fact, some sort of catastrophic event, can certainly assist them in the deployment and addressing any kind of concerns.

Mr. GREEN. Let me speak on behalf of probably a good portion of the American population when I say to you it is perceived that when the local government fails and the State government fails, it is perceived that the Federal Government should prevail. It is also perceived that in Louisiana, in New Orleans when the local and State did not step up to the plate, the Federal Government to a great extent, the level of participation was observation immediately after the catastrophe. It seems that there should be a plan in place when it comes to health care, food, water, justice system, and communications.

There should be some plan that the Federal Government has when local and State government can't deliver. There are things that happen that will cause local and State government to be ineffective. At this point, the Federal Government has to become efficacious. I am not hearing about the plan that the Federal Govern-

ment has when the State government can't step up and the local government can't, when they can't. Do you have something that is the equivalent of the MASH units, the Mobile Army Surgical Hospitals? Do you have the equivalent of some sort of mobile distribution system that is already in place and can be dispatched quickly? Do you have boots that can go on the ground immediately to give us that law and order that we finally saw in about day five, six, seven in Louisiana?

Do we have a food distribution system that is in place in the event a State and local government can't deliver? Is that plan in place? If that plan is in place, my assumption is it is linked to some sort of network within various States so that it can be an effective plan. Mr. Baker, could you kindly respond, please?

Mr. BAKER. If I could give you a short answer, it is we have plans to provide all of those things in support of State and local governments when they ask. We do not, in general, plan to take over from the State and local governments for obvious reasons. They rarely believe that they are going to suffer that kind of loss of control.

Mr. GREEN. Okay. Mr. Baker, with all due respect, and I appreciate what you are saying about the sovereignty, if you will, of the State government. I appreciate it. But we are talking about something now on a massive scale. God forgive that it would ever happen, hope that it won't happen, but let's assume that the State government is ineffective because it has been damaged severely. You must be prepared to deliver at this point in my opinion.

Mr. BAKER. Since we can deliver on request, we can also deliver when we determine that it is necessary to do so. I just want to caution that States are quite concerned if we started to plan to take over.

Mr. GREEN. I don't want you to do so, but what I don't want to see is people on top of buildings with signs saying help me and the Federal Government flying over in planes and not helping. That is what I don't want to see. So there must be some means by which we never, ever, ever allow what happened in New Orleans to happen again. There must be some means by which we can prevent this. That is the plan that I am looking for.

Mr. BAKER. We share that hope.

Mr. GREEN. Do we share the plan?

Mr. BAKER. We have the capability. We are working on additional——

Mr. GREEN. I have the capability to do surgery with a certain amount of education, which I do not have right now. Okay.

Mr. BAKER. You are doing pretty well.

Mr. GREEN. What I want is to know that my government is using the capability that it has so that it can produce a product. Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you. We now recognize the gentlelady from New York, Ms. Lowey, for 5 minutes.

Mrs. LOWEY. Thank you very much, Mr. Chairman. Again Assistant Secretary Baker, we have been talking earlier in this hearing about communication problems that have plagued first responders in every emergency in the last 15 years. We have heard enough about Katrina. The fiscal year 2007 Homeland Security appropria-

tions bill included multiple provisions that I had the privilege of championing with the help of our good Chairman related to first responder communications. Included were several provisions on planning and backup systems to implement the global networks went down, as in New Orleans. Earlier this year the FCC ended the digital television transmission spectrum auction without receiving the minimum bid to build the D block spectrum that was reserved for public safety. Addressing these issues should be one of the Department's top priorities. Assistant Secretary Baker, I was interested to read the portion of your testimony that promoted reverse 9/11 and enhanced 9/11.

In New York, the State emergency management office has developed New York Alert, an all hazard Web-based alert and notification portal that can activate the emergency alert system and send blast fax, e-mail, text messages, phone calls, et cetera, to subscribers across the State or to customized groups. This sounds just like the communications network you are promoting that enhance resiliency. Correct?

Mr. BAKER. Yes.

Mrs. LOWEY. However, the Department has turned down requests to provide funding for this program. In fact, grant guidance for the FEMA Predisaster Mitigation Program explicitly excludes this type of program. I am really puzzled that one branch of DHS supports alert systems, but when it comes to providing funding another branch opposes it. Assistant Secretary Baker, can you tell me what you are doing to ensure communications resiliency and can you explain this?

Mr. BAKER. I am not familiar with the grant guidance that you are talking about. We are certainly supportive of New York's efforts to do the kinds of things that you are talking about.

Mrs. LOWEY. What does "supportive" mean? It is a good idea.

Mr. BAKER. It is a good idea. I would not say that we have failed to fund New York's efforts to respond to emergencies, to build homeland security programs across the board. The grants to New York City and State have been quite substantial for obvious reasons, because we think that they are under a substantial threat. Whether all of the grant programs are focused on new technologies or only some of them are available for that, I am not in a position to answer. But I will take a look at that and I will get back to you because, as I said in the testimony, and I have said here today, these new technologies are crucial for our ability to respond flexibly and show the resilience that the committee would like us to show and that we would like the citizens to be able to show.

Mrs. LOWEY. Well, I would appreciate you getting back to me, because the FEMA Predisaster Mitigation Program explicitly excludes this type of program, which is quite extraordinary to me. Thank you very much. Dr. Bailey, what lessons could DHS learn from AT&T to increase the likelihood that our communications networks will survive major incidents?

Ms. BAILEY. Wow. That is a loaded question. Well——

Mrs. LOWEY. Well, I think it is important. If we are talking about resilience and if we don't discuss the facts and we are not preparing and the chair, and I and many of us have been talking about this issue for 5, 6 years, yes.

Ms. BAILEY. Wow, lessons learned. Certainly the attention to—admitting up front that bad things will happen. I think Dr. Sheffi mentioned that early in one of his responses. Bad things happen all the time. So it is not just being prepared for the very rare but very severe, you know, devastating, you know, terrorist attack, but also the day-to-day nasty things that happen. The pool chemical warehouses that catch on fire and release chlorine gas, the train derailments and the like. All of those can in many ways be——

Mrs. LOWEY. I don't mean to interrupt, but I have a couple of seconds left.

Ms. BAILEY. Okay.

Mrs. LOWEY. But what from your procedures, from your technology, what could you teach not Assistant Secretary Baker, let's say what could you really show DHS and how do we get it done? You know, we have been having these hearings for years. The private sector knows they have to do it or else they are going to lose a lot of money. We are going to lose a lot of lives and money and everything else. So what could you teach us?

Ms. BAILEY. Wow. Well, certainly there are the physical threats as well as the cyber threats. We would be very interested, in fact we are sharing our approaches to cyber security, for example, with DHS to address both the prediction and prevention, which is surprisingly more significant of an opportunity than certainly AT&T ever expected until we started looking at the traffic profiles and realizing that there are signatures of attacks actually before they happen, and if you can leverage that signature, you can buy yourself planning time and preparation time that is extremely valuable to mitigate the impacts. So that is just one example of what AT&T can and would love to share with DHS in terms of our capabilities.

Mrs. LOWEY. My time is up, but I would hope that the expertise that AT&T has could be shared. In fact, I would hope we get to the point where DHS can be the initiator of some of this technology so we can all benefit, not that we want to compete with AT&T. But we thank you for your leadership. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. We now recognize the gentlelady from California, Ms. Harman, for 5 minutes.

Ms. HARMAN. Thank you, Mr. Chairman. I want to commend you for holding the hearing on this important subject and to make certain that those listening in know that the Subcommittee on Intelligence, which I chair, will hold another hearing on this subject in a few days. Steve Flynn, a noted author, will be one of our witnesses. I think it is very important that we consider resilience as we consider whether our steps to protect our homeland are adequate.

Ms. HARMAN. I also want to apologize to you and to our witnesses for not being here during their testimony. I had two other hearings at the same time, and my little body went to both of those and is now here, hoping to ask a few questions.

Finally, I want to welcome especially Mr. Southers, who hails from Los Angeles and who works for the Los Angeles World Airports. LAX is in my district's backyard. I surround LAX, and it also happens to be, as I am sure he said, one of the top terrorist targets in the United States with a history of prior attacks.

Make no mistake, if an airport is attacked in our future, it is more likely to be LAX than any other airport; and that gets my attention, and that is why mine is a very familiar voice in the halls of the LAX administrators, maybe a little too familiar. I stay up at night, worrying about what could happen to that airport and particularly worrying about threats posed by vehicle-borne explosives, which according to the RAND Corporation and to others who have looked at this is the most likely kind of threat that could occur at that airport.

So I applaud your effort, Mr. Southers, to move beyond the traditional role of airport security teams. Real-time intelligence is a crucial tool to protecting critical infrastructure such as LAX, and your airport randomized vehicle checkpoints, which I have noticed, since I go through them all the time, are praiseworthy.

Critical infrastructure protection units are probably very useful as well, but as you note in your testimony, it was RAND—which I just mentioned—4 years ago, which determined that curbside bombs, including large truck bombs, were the top test to LAX and to other major U.S. airports.

Seven airline terminals surround the horseshoe. It literally looks like a horseshoe that one drives around on two levels at LAX. Each terminal is often extremely crowded, with lines extending out the door. It is not hard to imagine what kind of mischief could occur. Yet, 13 years after Oklahoma City and 1 year after Glasgow, we are not ready.

So, in thinking about resilience, I want to urge you to make certain that this summer, as promised, LAX and LAWA will install vehicle barriers—probably similar to the large flower pots, these concrete flower pots, that adorn the Capitol—at the most vulnerable points in that horseshoe, both at the upper tier and at the lower tier.

I do not know if a vote has just been called. No. So my time is still limited. I only have about a minute and a half, but I wanted to give you a chance, Mr. Southers, or anyone else who would like to opine to add to what I have just said.

Finally, let me just get this in while Mr. Lungren is here. As he knows, we coauthored the Safe Ports Act. One of the unique features of that act was a resiliency plan. This committee has been thinking about this well ahead of this year, and it pleases me to hear that many of you are also thinking about it. So I did want to commend you.

Mr. Southers.

Mr. SOUTHERS. Congresswoman, first, I do want to say, thank you for your support. Your voice is always welcomed at the airport. It certainly has been what has initiated some movement on our part.

I am happy to say that the first phase of the bollard plan is going to go in this summer. In fact, I have personally walked the upper level myself. Despite some challenges with regard to the level of protection necessary, I can assure you that the rating of those bollards is going to withstand vehicles of the impact of the attacks we have seen around the world. We certainly do still share some of those issues with regard to people's being on the curbside, and we are trying to mitigate that as much as possible.

One of the things we are able to do is to work a little bit closer with TSA in getting more screeners in there, particularly at Southwest, at Tom Bradley and at Terminals 6 and 7, to get them inside. While they are outside, we have stepped up our K–9 explosive detection teams out there.

So we have got a presence. We also have more of a presence of our officers as well. So we are certainly aware of that.

It has been quite some time, as you mentioned. This summer, we look forward to moving forward not only with the terminals, but with LAX fuel and with some of the other gates around the airport that you have mentioned in the past. Those phases will all start this summer.

Ms. HARMAN. Well, I thank you for that answer.

My time has expired, but I would just add that there are vulnerable airports all around America. As we think about resiliency, that is a place we have to look.

I do commend you for your efforts, and I will be looking for those flower pots in the very near future.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

I would like to thank the witnesses for their valuable testimony and the members for their very excellent questions.

The members of the committee may have additional questions for you, and we will ask that you respond expeditiously in writing to these questions, as a couple of witnesses have already agreed to do.

Chairman THOMPSON. Hearing no further business, the committee stands adjourned.

[Whereupon, at 12:05 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE MIKE ROGERS OF ALABAMA FOR STEWART A. BAKER, ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY

IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)

Question 1. While the number of Border Patrol officers has doubled over the recent past to about 18,000, the number of ICE agents has remained relatively level at about 6,000.

Can the Department meet its immigration enforcement responsibilities with so few immigration agents?

Given the national emphasis on the importance of enforcement of immigration law, how many ICE agents does the Department need to function effectively?

Answer. The Department has requested increases in funding for Immigration and Customs Enforcement that support the administration's Secure Border Initiative (SBI), controlling the border and executing a comprehensive interior enforcement strategy. In the fiscal year 2009 request, the President requested $5.7 billion for ICE. The 2009 request includes resources for 87 Office of Investigations (OI) Special Agents and 44 positions for the Visa Security Program and the Office of Professional Responsibility (OPR), as well as increases for detention beds and State and local law enforcement coordination.

In addition, 74 positions along with 1,000 additional beds have been requested for ICE's Office of Detention and Removal Operations (DRO) in order to deal with removal costs required to meet current demand and the demand generated by increased enforcement activities associated with SBI and special authority granted to State and local law enforcement officers under Section 287(g) of the Immigration and Nationality Act. These positions included 20 Deportation Officers, 40 Immigration Enforcement Agents, 8 Deportation Assistants and 6 support positions.

The number of authorized positions for DRO has nearly doubled from approximately 4,000 positions in fiscal year 2005 to 7,734 positions in fiscal year 2008. It is also important to note that the Criminal Alien Program (CAP) was transferred from the OI to DRO, and the Office of International Affairs (OIA), which had been a part of OI, is now a stand-alone entity within ICE. Despite the realignment of these resources, OI still maintains approximately 6,000 Special Agents nationwide.

As a result of increased funding over the past several fiscal years, ICE has achieved many successes. In fiscal year 2007, for example, ICE's investigative and detention and removal accomplishments include:

- Enhanced Immigration Enforcement: Initiated 1,093 worksite enforcement investigative cases, which resulted in 863 criminal arrests (compared to 716 in fiscal year 2006) and 4,077 administrative arrests.
- Increased Compliance Enforcement: ICE implemented a high-intensity compliance enforcement operation to detect, deter, and disrupt terrorist operatives who sought to exploit the non-immigrant process in order to remain illegally in the United States. The operation resulted in 249 completed investigations and 73 arrests.
- Increased Human Smuggling Investigations: ICE initiated 2,528 human smuggling investigative cases, which resulted in 1,821 criminal arrests, 1,150 indictments, 1,209 convictions, and seized $16,400,283 in related monetary instruments.
- Apprehended Sexual Predators of Children: ICE achieved a total of 10,434 criminal and administrative arrests through Operation Predator.
- Increased Commercial Fraud and Intellectual Property Rights Investigations: ICE initiated 1,275 Commercial Fraud and Intellectual Property Rights investigative cases, which resulted in 246 criminal arrests, 178 indictments, and 196 convictions.

- Targeted Transnational Gangs: ICE arrested a total of 3,302 gang members and associates Nation-wide.
- Furthered Nation-wide Document-Fraud Prevention Efforts: ICE initiated 1,309 fraud investigations, leading to a record 1,531 arrests and 1,178 convictions.
- Strengthened Border Enforcement Security Task Forces (BESTs): Task Forces collectively made 516 criminal arrests, 1,037 administrative arrests, seized over 49,552 pounds of marijuana, 1,326 pounds of cocaine, 151 pounds of methamphetamine, 135 pounds of heroin, 237 weapons, 12 explosives, and approximately $2.5 million in U.S. currency.
- Enforcement Against Visa Violators: ICE investigators worked to ensure compliance with the Nation's immigration laws among student and exchange visitors and other nonimmigrant visitors to the United States. ICE arrested 1,558 high-risk, non-immigrant status violators.
- Visa Security Program: ICE expanded overseas deployment to nine visa security posts in eight countries and trained more than 40 Special Agents to serve as visa security officers. ICE investigations through this program resulted in the denial of more than 750 visas and the initiation of more than 140 investigations.
- Set New Record for Alien Removals: ICE removed more than 276,000 illegal aliens, including voluntary removals, from the country—a record for the agency and a 45 percent increase over the number of removals during the prior fiscal year.
- Removed Criminal Aliens: ICE initiated removal proceedings against 164,296 criminal aliens encountered in U.S. jails and prisons, which exceeds the Criminal Alien Program fiscal year 2006 total by over 140 percent.
- Leveraged Alternatives to Detention: ICE processed 8,300 non-detained aliens through the Alternatives to Detention program, including 1,989 Intensive Supervision Appearance Program participants and approximately 6,300 Electronic Monitoring Program participants.
- Increased Fugitive Operations Team Arrests: ICE added an additional 23 Fugitive Operation Teams, for a total of 75, which arrested over 30,000 illegal aliens. ICE processed and eliminated more than 100,000 fugitive alien cases and reduced the backlog of fugitive cases for the first time in history.
- Increased Removal Process Efficiencies: ICE's Detention Enforcement and Processing Offenders by Remote Technology (DEPORT) Center made it possible to identify and screen criminal aliens incarcerated in Federal prisons to ensure their removal upon the completion of their sentences. ICE also deployed the Electronic Travel Document System to all 24 ICE DRO Field Offices and consulates of Guatemala, Honduras, and El Salvador, decreasing the number of days required to issue travel documents from 14 days to 6 days.
- Initiated Significant Financial Investigations: ICE initiated 3,069 financial investigations, resulting in 1,394 arrests and 897 convictions.
- Increased Number of Trade Units: To combat trade-based money laundering, ICE now has Trade Transparency Units (TTUs) in place in Colombia, Paraguay, Argentina, and Brazil. In fiscal year 2007, ICE TTUs initiated 95 trade-based money laundering investigations and generated 36 investigative referrals.
- Increased Arms and Strategic Technology Investigations: ICE increased its arms and strategic technology investigations, resulting in 186 arrests (compared to 144 in fiscal year 2006), 178 indictments, and 115 convictions.

Question 2. In my home State of Alabama, a number of county sheriffs have reported a complete lack of response on ICE's part to dealing with detained illegal aliens. I understand that this is due to inadequate numbers of Detention and Removal Officers, and insufficient bed space.

How does the Department plan to deal with this growing inability to handle the increasing number of immigrant detainees?

Answer. In the past 3 fiscal years, the administration has substantially increased ICE resources. As I outlined in detail in my response above, the President requested $5.7 billion for ICE in his fiscal year 2009 budget, which represents an increase of approximately 12 percent over fiscal year 2008, excluding emergency funding provided by Congress. Program increases total over $160 million and target the priority areas of this administration to allow ICE to be a highly valuable contributor to the Secure Border Initiative (SBI), enforce customs laws critical to the Nation's security, and ensure we are protecting the American public. ICE has made tremendous progress in immigration enforcement through greater innovation with its resources combined with more effective oversight.

In Alabama, there are a total of 89 recognized facilities. All Federal and State facilities, as well as seven county facilities have 100 percent screening by ICE. The remaining 74 county and city facilities receive limited coverage. In fiscal year 2008,

Congress provided funding for an additional Criminal Alien Program (CAP) team for Montgomery, Alabama. This CAP team is in the process of being hired and deployed to Montgomery, Alabama. Since September 10, 2003, ICE has had a Memorandum of Agreement (MOA) with the Alabama Department of Public Safety. In addition, three other Alabama law enforcement agencies (the Prattville Police Department, the Etowah County Sheriff's Office, and the Huntsville Police Department) have all applied for 287(g) Delegation of Authority. These applications are currently pending.

To continue to improve our responsiveness to States and localities, ICE has developed Secure Communities, A Comprehensive Plan to Identify and Remove Criminal Aliens. In order to ensure no criminal alien is released into the community due to lack of detention space, ICE must expand its number of available beds to cover increased detention needs generated by the plan. The fiscal year 2008 Appropriation provided ICE with $200 million to develop this plan, and approved an increase of 4,500 detention beds for an annual average daily population of 32,000. ICE uses a detention space management model to help determine where detention space should be added. As the plan is implemented, ICE will review bed detention needs.

Secure Communities consists of the following strategic goals:

- *Strategic Goal 1.*—Identify and process all criminal aliens amenable for removal while in Federal, State, and local custody;
- *Strategic Goal 2.*—Enhance current detention strategies to ensure no removable criminal alien is released into the community due to a lack of detention space or an appropriate alternative to detention;
- *Strategic Goal 3.*—Implement removal initiatives that shorten the time criminal aliens remain in ICE custody prior to removal, thereby maximizing the use of detention resources and reducing cost; and
- *Strategic Goal 4.*—Maximize cost effectiveness and long-term success through deterrence and reduced recidivism of criminal aliens returning to the United States.

Question 3a. One of my concerns is the nature of the training that ICE agents receive in customs and immigration. In my State of Alabama, many agents work customs at the ports, but very few are available for immigration matters. If we split the training to have some agents focus on customs and others specialize in immigration, it would seem there would be more officers to handle immigration enforcement.

Do all incoming agents receive the same training, or do they specialize in one area or the other?

Answer. While U.S. Customs and Border Protection (CBP) works to secure the Nation's borders at and between the official ports of entry, ICE Special Agents are responsible for investigating a range of issues that may threaten national security within the interior of the United States. Both agencies work closely to secure our homeland. Additionally, by bringing together customs and immigration enforcement, DHS can fight crime and terrorist activity in ways not possible before the founding of DHS. Investigators on immigration cases can track the money trails that support smuggling and document fraud operations. Financial investigators can use immigration violations to build cases against criminals. ICE brings all of its powerful authorities to bear on all cases, requiring agents to be sufficiently trained on all of those authorities. Accordingly, all ICE Special Agents receive instruction in both customs and immigration law, and are trained to enforce both.

Question 3b. What about agents who were working prior to the merger that created ICE in March 2003?

Answer. Special Agents hired prior to the merger were cross-trained in one of two approved programs. The program for Customs Agents provided immigration law/enforcement practices and program for Immigration Agents provided customs law/enforcement practices. Every Agent in the agency was required to take and successfully be tested in the requisite cross-training program.